(19)日本国特許庁（ＪＰ）　(12) **公表特許公報**（Ａ）　(11)特許出願公表番号
特表2002－521879
（P2002－521879A）
(43)公表日　平成14年７月16日(2002.7.16)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*(参考)
Ｈ０４Ｌ　9/08		Ｇ０９Ｃ　1/00	６４０Ｚ	５Ｃ０６４
Ｇ０９Ｃ　1/00	６４０	Ｈ０４Ｎ　7/20	６３０	５Ｊ１０４
Ｈ０４Ｎ　7/20	６３０		ＺＥＣ	
	ＺＥＣ	Ｈ０４Ｌ　9/00	６０１Ｃ	
			６０１Ａ	

審査請求　未請求　　予備審査請求　有　　（全 54 頁）　　最終頁に続く

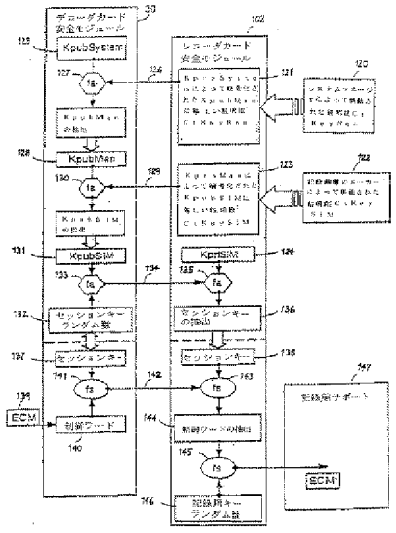
(21)出願番号　特願2000－560729(P2000－560729)
(86)(22)出願日　平成11年７月14日(1999.7.14)
(85)翻訳文提出日　平成13年１月15日(2001.1.15)
(86)国際出願番号　ＰＣＴ／ＩＢ９９／０１３２３
(87)国際公開番号　ＷＯ００／０４７１８
(87)国際公開日　平成12年１月27日(2000.1.27)
(31)優先権主張番号　９８４０１７７８．０
(32)優先日　平成10年７月15日(1998.7.15)
(33)優先権主張国　欧州特許庁（ＥＰ）
(31)優先権主張番号　９８４０１８７０．５
(32)優先日　平成10年７月22日(1998.7.22)
(33)優先権主張国　欧州特許庁（ＥＰ）

(71)出願人　カナル　プラス　ソシエテ　アノニム
フランス国　エフ－75711　パリ　セデックス　15　クアイ　アンドレ　シトロエン　85／89
(72)発明者　ダウボイス，ジャン－ラック
フランス国　エフ－75116　パリ　リュ　ユージン　マニュエル　19
(72)発明者　ベナルデウ，クリスチャン
フランス国　エフ－77600　セイント　ジョージス　アレ　デス　プイサティアス　13
(74)代理人　弁理士　斉藤　武彦　（外１名）

最終頁に続く

(54)【発明の名称】　複数のディジタルオーディオビジュアル装置間での安全な情報通信のための方法および装置

(57)【要約】
本発明は、少なくとも第１および第２のディジタルオーディオビジュアル装置（３０，５２）間で安全な情報通信を行い、第１の装置（３０）が管理私用鍵ＫｐｒｉＭａｎによって暗号化されたトランスポート公開鍵ＫｐｕｂＴを含む証明証Ｃｔ（ＫｐｕｂＴ）を第２の装置（５２）に通信し、第２の装置（５２）が等しい管理公開鍵ＫｐｕｂＭａｎを使用して証明証を暗号解読し、その後トランスポート公開鍵ＫｐｕｂＴを使用して第１の装置に送信された情報を暗号化し、第１の装置が等しい私用鍵ＫｐｒｉＴを使用してこの情報を暗号解読することを特徴とする方法に関するものである。本発明は、特に第１および第２のデコーダ間で安全な通信を行う方法に応用可能である。



【特許請求の範囲】

【請求項１】　少なくとも第１および第２のディジタルオーディオビジュアル装置間で安全な情報通信を行う方法であって、かつ前記第２の装置が、管理私用鍵で暗号化されたトランスポート公開鍵を含む証明証を受信し、前記第２の装置が、等しい管理私用鍵を使用して前記証明証を暗号解読し、その後前記トランスポート公開鍵を使用して前記第１の装置に送信された情報を暗号化し、前記第１の装置が等しい私用鍵を使用して前記情報を暗号解読することを特徴とする少なくとも第１および第２のディジタルオーディオビジュアル装置間で安全な情報通信を行う方法。

【請求項２】　前記トランスポート私用／公開鍵対が、前記第１および第２の装置に特に関連していることを特徴とする請求項１記載の方法。

【請求項３】　前記第２の装置によって送信された前記暗号化情報がセッション鍵を含むことを特徴とするいずれかの前述の請求項に記載の方法。

【請求項４】　前記セッション鍵が前記第２の装置によって生成され、かつ対称暗号化アルゴリズムで使用可能である鍵であることを特徴とする請求項３に記載の方法。

【請求項５】　前記セッション鍵が、その後に前記第２の装置に通信された制御ワード情報を暗号化するために前記第１の装置によって使用されることを特徴とする請求項３あるいは４に記載の方法。

【請求項６】　前記第２の装置が、前記等しいセッション鍵を使用して制御ワード情報を暗号解読し、その後この制御ワードに関連したスクランブル伝送のセクションをデスクランブルすることを特徴とする請求項５に記載の方法。

【請求項７】　前記第１および第２の装置がそれぞれの第１および第２のポータブルセキュリティモジュールを含むことを特徴とするいずれかの前述の請求項に記載の方法。

【請求項８】　前記第２の装置が、システム私用鍵によって暗号化された前記管理公開鍵を含むシステム証明証を受信し、前記第２の装置が、その後前記暗号化トランスポート公開鍵を暗号解読するために使用される前記管理公開鍵を得るためにシステム公開鍵を使用して前記システム証明証を暗号解読することを特

徴とするいずれかの前述の請求項に記載の方法。

【請求項９】　前記第１の装置と前記第２の装置との間の前記通信リンクがバス接続によって実現されることを特徴とするいずれかの前述の請求項に記載の方法。

【請求項１０】　前記第１および第２のディジタルオーディオビジュアル装置が第１および第２のデコーダを含むことを特徴とするいずれかの前述の請求項に記載の方法。

【請求項１１】　前記第１および第２のデコーダがディジタルテレビジョン伝送を受信するように構成されていることを特徴とする請求項１０に記載の方法。

【請求項１２】　前記第１および第２のディジタルオーディオビジュアル装置がデコーダ装置およびレコーダ装置を含むことを特徴とする請求項１から９までのいずれかに記載の方法。

【請求項１３】　デコーダ装置とレコーダ装置との間で安全な情報通信を行う方法であって、かつ前記装置の中の第１の装置が、管理私用鍵によって暗号化された装置公開鍵を含む証明証を前記第２の装置に通信し、前記第２の装置が、等しい管理私用鍵を使用して前記証明証を暗号解読し、その後前記トランスポート公開鍵を使用して前記第１の装置に送信された情報を暗号化し、前記第１の装置が等しい私用鍵を使用して前記情報を暗号解読することを特徴とするデコーダ装置とレコーダ装置との間で安全な情報通信を行う方法。

【請求項１４】　前記第１の装置が、システム私用鍵によって暗号化された前記管理公開鍵を含むシステム証明証を前記２の装置に通信し、前記第２の装置が、その後前記暗号化トランスポート公開鍵を暗号解読するために使用される前記管理公開鍵を得るためにシステム公開鍵を使用して前記システム証明証を暗号解読することを特徴とする請求項１３に記載の方法。

【請求項１５】　前記トランスポート私用／公開鍵対が、前記第１および第２の装置に特に関連していることを特徴とする請求項１３あるいは１４に記載の方法。

【請求項１６】　前記管理私用／公開鍵対が、前記第１の装置の供給者と特

に関連していることを特徴とする請求項１３～１５のいずれかに記載の方法。

【請求項１７】　前記管理私用／公開鍵対が、前記第２の装置の供給者と特に関連していることを特徴とする請求項１４に記載の方法。

【請求項１８】　前記第２の装置によって送信された前記暗号化情報がセッション鍵を含むことを特徴とする請求項１３～１７のいずれかに記載の方法。

【請求項１９】　前記セッション鍵が前記第２の装置によって生成され、かつ対称暗号化アルゴリズムで使用可能である鍵であることを特徴とする請求項１８に記載の方法。

【請求項２０】　前記セッション鍵が、その後に前記レコーダ装置に通信された制御ワード情報を暗号化するために前記デコーダ装置によって使用されることを特徴とする請求項１８あるいは１９に記載の方法。

【請求項２１】　前記レコーダ装置が、前記等しいセッション鍵を使用して前記制御ワード情報を暗号解読し、その後記録暗号化鍵を使用して前記制御ワード情報を再暗号化でき、前記再暗号化制御ワード情報が、この制御ワード情報に関連したスクランブル伝送データとともに記録支持媒体に前記レコーダ装置によって記憶されることを特徴とする請求項２０に記載の方法。

【請求項２２】　前記レコーダ装置が記録暗号化鍵のコピーを前記デコーダ装置に通信することを特徴とする請求項２１に記載の方法。

【請求項２３】　前記レコーダ装置が前記セッション鍵によって暗号化されるとき前記記録暗号化鍵のコピーを通信することを特徴とする請求項２２に記載の方法。

【請求項２４】　前記レコーダ装置およびデコーダ装置の少なくとも１つが少なくとも１つの携帯セキュリティモジュールを含むことを特徴とする請求項１３から２３までのいずれかに記載の方法。

【請求項２５】　前記第１の装置がレコーダ装置に対応し、かつ前記第２の装置がデコーダ装置に対応することを特徴とする請求項１３から２４までいずれかに記載の方法。

【請求項２６】　前記デコーダ装置がディジタルテレビジョン伝送を受信するように構成されていることを特徴とする請求項１３から２５までのいずれかに

記載の方法。

【請求項２７】　実質的にここに記載されているような少なくとも第１および第２のディジタルオーディオビジュアル装置間で安全な情報通信を行う方法。

【発明の詳細な説明】

【０００１】

本発明は、ネットワークで接続された複数のディジタルオーディオビジュアル装置間で安全な情報通信を行う方法および装置に関するものである。

【０００２】

本発明は、スクランブルオーディオビジュアル情報が多数の加入者に放送されるディジタルテレビジョンの分野に特に応用可能であり、各加入者は、その後に見るための伝送プログラムをデスクランブルできるデコーダあるいは統合受信機／デコーダ（ＩＲＤ）を所有する。

【０００３】

典型的なシステムでは、スクランブルディジタルオーディオビジュアルデータは、ディジタルデータをデスクランブルするための制御ワードとともに伝送され、制御ワードそのものは、利用鍵によって暗号化され、暗号化形式で伝送される。暗号化制御ワードを暗号解読し、その後伝送データをデスクランブルするために利用鍵の等価物を使用するデコーダは、スクランブルディジタルデータおよび暗号化制御ワードを受信する。支払済加入者は、特定のプログラムの視聴を可能にするように暗号化制御ワードを暗号解読するのに必要な利用鍵を周期的に受信する。暗号化鍵および暗号解読鍵は、従来はデコーダを個人の専有にするために使用されるスマートカードのような携帯セキュリティモジュールに記憶される。

【０００４】

既存の加入管理システムはしばしば同じアドレスで同じ人のための第２の加入を許す際に難点を有するので、２つあるいはそれ以上のデコーダを有するユーザの場合に特定の問題が生じる。したがって、このような状況では、２つあるいはそれ以上のデコーダが同じ加入を使用して作動できることは有利である。

【０００５】

ニューズデータコム社（Ｎｅｗｓ　Ｄａｔａｃｏｍ　Ｌｉｍｉｔｅｄ）の名義のＰＣＴ特許出願ＷＯ９７／３５４３０号はこの問題に対する１つの可能な解決策を示している。このシステムでは、一対のデコーダはマスタ／スレーブ構成で構成される。加入権は、マスタデコーダおよびその関連スマートカードによって

管理される。加入権をスレーブデコーダに転送するために、スレーブスマートカードは、マスタデコーダに一定の間隔で挿入されねばならない。このシステムの欠点は、ユーザがスレーブデコーダのカードを手動で引き抜き、再装填し、取り換えることを余儀なくされるということである。

【０００６】

他の提案された解決策は、マスタスマートカードにあるのと全く同じ権利を含む複製スマートカードの生成を含んだ。複数のデコーダに全く同じ権利を与えることは望ましくないかもしれなく、クローンあるいは複製のカードの作成は常にリスク詐欺を招くので、このような解決策も望ましくない。

【０００７】

ディジタルシステムで伝送されたデータに関連した他の特定の問題は、無損失の品質を有する再生の容易さにある。デスクランブルプログラムは標準ＶＣＲによって視聴し、記録するためのアナログリンク（例えば、「ペリテル」リンク）を介して送られる場合、この品質は、標準アナログカセット記録に関連した品質よりも大きくないままである。

【０００８】

対照として、直接ディジタルリンクによって新しい世代のディジタル記録装置（例えば、ＤＶＨＳあるいはＤＶＤレコーダ）の１つに送られる任意のデスクランブルディジタルデータは、最初に伝送されたプログラムと同じ品質のものであるので、少しの画質あるいは音質の低下もなしに任意の回数再生できる。したがって、記録済デスクランブルデータは海賊コピーを作成するためにマスタ記録として使用されることはかなりのリスクがある。

【０００９】

フランス特許出願９５０３８５９号は、この問題を解決する１つの方法を示している。このシステムでは、デスクランブルディジタルデータは、決してディジタル記録媒体に記録されない。その代わりに、この出願に記載されたデコーダは、記録のためのデータをスクランブル形式で支持媒体に転送する。データをデスクランブルするのに必要な制御ワードは、他の鍵によって再暗号化され、スクランブルデータとともに記録支持体に記憶される。この新規の鍵は、受信機／デコ

ーダにだけ既知であり、プログラムを視聴するための制御ワードを得るのに必要とされる利用鍵に取って代わる。

【００１０】

このようなシステムの長所は、データが決して「暗号化されていない」形式で記憶されなく、デコーダに記憶された新規の鍵を所有しないで見ることができないことである。このシステムは、利用鍵は毎月変更するので、ディジタルテープに登録された制御ワードを再暗号化するためのデコーダによって選択された鍵の使用がデコーダが加入月の終了後さえテープに記録された制御ワードをなお暗号解読できることを意味するという長所もある。

【００１１】

この前述の特許出願に提案されたシステムの短所は、記録がこの特定のデコーダでのみ見ることができるということである。このデコーダが故障するかあるいは取り換えられる場合、記録はもはや再生できない。同様に、システムでデコーダを接続しないでディジタルレコーダで直接記録を再生できない。

【００１２】

デコーダおよびレコーダがより効率的に作動できるために、装置間に安全化あるいは暗号化された通信リンクを備えることは望ましい。上記の説明から分かるように、デコーダおよびレコーダの相互作用は、例えば、スクランブル伝送が記録されるが、デコーダだけがこのような伝送を暗号解読するのに必要な情報を所有している場合、問題をもたらすかもしれない。装置間に安全なリンクを実現することによって、記録を作成するかあるいは再生するのに必要な情報は装置間に自由に送ることができる。

【００１３】

一般的な実施形態および特定の実施形態における本発明の目的は、これらの従来技術のシステムの問題のいくつかあるいは全てを解決することにある。

【００１４】

本発明によれば、少なくとも第１および第２のディジタルオーディオビジュアル装置間で安全な情報通信を行い、かつ第２の装置が、管理私用鍵で暗号化されたトランスポート公開鍵を含む証明証を受信し、第２の装置が、等しい管理私用

鍵を使用して証明証を暗号解読し、その後前記トランスポート公開鍵を使用して第１の装置に送信された情報を暗号化し、第１の装置が等しい私用鍵を使用して情報を暗号解読することを特徴とする方法を提供する。

【００１５】

このような方法では、第１の装置は、管理私用鍵を使用して生成された証明証で個人の専有とされるマスタ装置の役割を引き受けることができる。この管理私用鍵は、システムマネージャによって秘密に保有され、証明証に記憶された情報から得られなくてもよい。第２の装置はスレーブ装置の役割を引き受けることができる。第２の装置によって保有されたトランスポート公開鍵によって暗号解読された情報は、第１の装置によって保有された等しい私用鍵によってだけ暗号解読されてもよい。後述されるように、この情報はその後、安全な両方向リンクを生じさせ、加入権および他の情報を転送するために使用されてもよい。

【００１６】

有利なことには、トランスポート私用／公開鍵対は特に第１および第２の装置対に関連している。これは、第１の装置に伝送された全暗号化メッセージのセキュリティを保証する。

【００１７】

理解されるように、独自の鍵の使用はセキュリティのレベルの増加を可能にするが、このような複写に関連したセキュリティリスクが比較的低い場合、例えば、異なる地域で分散された異なる対の装置に対して非独自の鍵を使用することがいくつかの場合に決定されてもよい。

【００１８】

好ましくは、第２の装置によって送信された暗号化情報は、セッション鍵、特に第２の装置によって生成され、対称暗号化アルゴリズムで使用可能であるセッション鍵を含む。加入の転送のための通信セッションの開始で生成されてもよいこの鍵は、その後第１の装置と第２の装置との間での両方向情報通信のために使用できる。

【００１９】

他の実施形態では、非対称アルゴリズムの私用／公開鍵対に対応するセッショ

ン鍵対が使用されてもよい。

【００２０】

変更可能な対称セッション鍵の長所は、このような鍵が提供する増加されたセキュリティのレベルならびに可能にする両方向通信の可能性にある。それにもかかわらず、例えば、伝送関連情報が第２の装置によって保有されたトランスポート公開鍵を使用して直接に暗号化される他の実施形態が可能である。

【００２１】

１つの実施形態では、セッション鍵は、その後第２の装置に通信された制御ワード情報を暗号化するために第１の装置によって使用される。このような実施形態では、第２の装置は、等しいセッション鍵を使用して制御ワード情報を暗号解読し、その後関連伝送あるいは表示するためのプログラムをデスクランブルする。

【００２２】

１つの実施形態では、第１の証明証の通信前に、第２の装置は、システム私用鍵によって暗号化された管理公開鍵を含む二次システム証明証を受信し、第２の装置は、その後暗号化トランスポート公開鍵を暗号解読するために使用される管理公開鍵を得るためにシステム公開鍵を使用してシステム証明証を暗号解読する。

【００２３】

この実施形態は、例えば、第１および第２の装置に対して異なる供給者が存在する場合、実施されてもよい。このシステム公開鍵は、例えば、第２の装置の供給者によって秘密に保有されてもよい。第２の装置の供給者が第１の装置の供給者のセキュリティの保全性を確信している場合、システム証明証が発行されるだけである。その後、指定された第１の装置の供給者は、第２の装置のスマートカードがこのようなカードの出所を認証できるように全ての第１の装置のスマートカードにこの証明証を埋め込む。

【００２４】

理解されるように、第２の装置の供給者は、システム証明証を生成するために第１の装置の供給者の管理公開鍵だけを知る必要があり、どちらの当事者もこれ

らの認証動作を実行する際に私用暗号化鍵を共用する必要がない。

【００２５】

装置間の安全な通信リンクは、伝送をデスクランブルすることに関する異なる情報あるいは他の題材さえ含む多数の異なる種類の情報を伝達するために使用されてもよい。特に、上記の実施形態は、制御ワード情報の暗号化および通信でのセッション鍵の使用を検討しているが、他の実施形態が可能である。例えば、記録されるオーディオおよび／またはビジュアルデータは、セッション鍵を使用して第１の装置によって直接暗号化され、暗号解読および表示のために第２の装置に直接通信されてもよい。

【００２６】

他の実施形態は、例えば、第２の装置が制御ワード情報を暗号解読し、第１の装置と同じ方法で伝送をデスクランブルするために全ての動作を実行できるように第１の装置にある利用鍵を転送するために安全な通信リンクを使用してもよい。

【００２７】

上記の説明は第１および第２の装置に関する暗号化動作および暗号解読動作を説明しているが、これらの動作および特にこのような動作に必要とされる鍵は、必ずしも装置そのものに永久に統合される要素によって管理あるいは保有される必要がないことを理解すべきである。

【００２８】

特に、好ましい実施形態では、第１および第２の装置は、前述の暗号化ステップあるいは暗号解読ステップのいくつかあるいは全てを実行するために使用される第１および第２の携帯セキュリティモジュールをさらに含む。

【００２９】

このような携帯セキュリティ装置は、この装置の物理サイズおよび特性に応じて任意の便宜的な形をとることができる。例えば、いくつかの場合、銀行カードと同等なスマートカードが使用されてもよいが、ＰＣＭＣＩＡ型式カードのような他のフォーマットが同様に可能である。

【００３０】

２つの装置間の物理的通信リンクは、多数の形式、例えば、ラジオ、電話あるいは赤外線リンクをとってもよい。しかしながら、好ましくは、通信リンクは、バス、例えばＩＥＥＥ１３９４バスリンク上の第１および第２のデコーダの接続によって実現される。

【００３１】

本発明は第１および第２の装置を参照して説明されているが、同じ原理が一連の装置間、例えば、単一マスタ装置と複数のスレーブ装置との間で一連の通信を生じさせるために使用されてもよい。

【００３２】

本発明は、特に第１および第２のデコーダ間での安全な通信リンクの実現に応用可能であるが、排他的に第１および第２のデコーダ間での安全な通信リンクの実現に応用可能でない。しかしながら、他のディジタルオーディオビジュアル装置と併用するための本発明の他の応用は、例えば、２つのディジタルＶＣＲ等間でデコーダからディジタルＶＣＲへの情報を暗号化することを思い描いてもよい。

【００３３】

１つの好ましい実施形態では、この装置はデコーダ装置およびレコーダ装置を含んでもよい。したがって、本発明は、デコーダ装置とレコーダ装置との間で安全な情報通信を行い、かつ前記装置の中の第１の装置が、管理私用鍵によって暗号化された装置公開鍵を含む証明証を第２の装置に通信し、第２の装置が、等しい管理私用鍵を使用して証明証を暗号解読し、その後前記トランスポート公開鍵を使用して第１の装置に送信された情報を暗号化し、第１の装置が等しい私用鍵を使用して前記情報を暗号解読することを特徴とする方法に及ぶ。

【００３４】

このような方法では、通信を開始する第１の装置は、管理私用鍵によって生成される証明証で個人の専用とされる。管理私用鍵は、この装置の責任を負う供給者（例えば、レコーダ装置メーカー）によって秘密に保有され、証明証に記憶された情報から得られなくてもよい。したがって、このような証明証の通信は、第２の装置に通信を開始する装置のＩＤおよび出所に関する保証レベルを与える。

【００３５】

さらに、第２の装置によって保有される装置公開鍵によって暗号化された情報は、第１の装置によって保有される等しい私用鍵によってだけ暗号解読されてもよく、それによって第２の装置は第１の装置に秘密情報で通信できる。後述されるように、この情報はその後、安全な両方向リンクを生じさせるために使用されてもよい。

【００３６】

好ましくは、第１の装置証明証の通信前、第１の装置は、システム私用鍵によって暗号化された管理公開鍵を含むシステム証明証を第２の装置に通信し、第２の装置は、その後装置証明証を暗号解読するために使用される管理公開鍵を得るためにシステム公開鍵を使用してシステム証明証を暗号解読する。

【００３７】

私用システム鍵は、例えば、第２の装置の供給者（例えば、デコーダの責任を負う放送システムマネージャ）によって秘密に保有されてもよい。第２の装置の供給者が第１の装置の供給者でのセキュリティの保全性を確信する場合、すなわち第２の装置が、管理私用鍵が第１の装置の供給者によってのみ既知であることおよび必要な手段がこの鍵を秘密にするために適当に与えられることを確信する場合、システム証明証だけが発行される。

【００３８】

理解されるように、第２の装置の供給者は、システム証明証を生成するために第１の装置の供給者の公開管理鍵だけを知る必要があり、どちらの当事者もこれらの証明動作を実行する際にその私用暗号化鍵を共用する必要がない。

【００３９】

有利なことには、装置私用／公開鍵対は特に第１の装置に関連している。これは第１の装置に伝送された全暗号化メッセージのセキュリティを保証する。さらに有利なことには、管理私用／公開鍵対は、特に第１の装置の供給者に関連し、システム私用／公開鍵対（ある場合）は特に第２の装置の供給者に関連する。

【００４０】

理解されるように、独自の鍵の使用はセキュリティのレベルの増加を可能にす

るけれども、いくつかの場合、非独自の鍵を使用することが決定されてもよい。例えば、第１の装置の大量生産の場合、このような複製に関連したセキュリティリスクは比較的低いので、このような装置が異なる地域に分散されたならば、これらの装置の中のいくつかは同じ装置の私用鍵を共用してもよい。

【００４１】

好ましくは、第２の装置によって送信された暗号化情報は、セッション鍵、特に第２の装置によって生成され、対称暗号化アルゴリズムで使用可能なセッション鍵を含む。記録セッションの開始で生成されてもよいこの鍵は、その後第１および第２の装置間での両方向情報通信のために使用できる。

【００４２】

他の実施形態では、非対称アルゴリズムの私用／公開鍵対に対応するセッション鍵対が使用されてもよい。

【００４３】

変更可能なセッション鍵の長所は、このような鍵が与える増加されたセキュリティのレベルならびに対称セッション鍵が選択される場合にこのような鍵が可能にする安全な両方向通信の可能性にある。それにもかかわらず、記録動作に関連した情報が第２の装置によって保有される装置公開鍵を使用して直接暗号化されてもよい他の実施形態が可能である。

【００４４】

１つの実施形態では、セッション鍵は、デコーダ装置によってレコーダ装置にその後に通信される制御ワード情報を暗号化するために使用される。このような実施形態では、レコーダ装置は、等しいセッション鍵を使用して制御ワード情報を暗号解読し、その後記録暗号化鍵を使用して制御ワード情報を再暗号化してもよく、再暗号化制御ワード情報は、この制御ワード情報に関連したスクランブル伝送データとともに記録支持媒体上にレコーダによって記憶される。

【００４５】

レコーダ装置によって保有される記録鍵を使用して制御ワード情報の暗号化によって、レコーダ装置は、伝送を受信し、転送するために最初に使用されるデコーダ装置とは無関係に記録済スクランブル伝送をいつでも再生できる。

【００４６】

有利なことには、レコーダ装置は記録暗号化鍵のコピーをデコーダ装置に通信する。これは通信前にセッション鍵によって便宜的に暗号化されてもよい。このコピーは、その後デコーダによって暗号解読され、記録鍵のバックアップ鍵はデコーダに記憶されてもよい。

【００４７】

理解されるように、安全な通信リンクは、多数の異なる種類の情報を伝達するために使用されてもよい。特に、上記の実施形態は記録動作で使用するための制御ワードの暗号化および通信でのセッション鍵の使用を検討しているが、他の実施形態が可能である。例えば、記録されるオーディオおよび／またはビジュアルデータは、セッション鍵を使用してデコーダによって直接暗号化され、記録前の暗号解読およびその後の再暗号化のためにレコーダに通信されてもよい。

【００４８】

他の実施形態は、例えば、レコーダ装置が記録支持媒体上への再暗号化あるいは再スクランブル形式でのその記録前に制御ワード情報を暗号解読するおよび／またはデスクランブルする全ての動作を実行できるようにデコーダ利用鍵をレコーダ装置に転送するために安全な通信リンクを使用してもよい。

【００４９】

上記の説明は、デコーダ装置あるいはレコーダ装置に関する暗号化動作を説明しているが、これらの動作および特にこのような動作に必要とされる鍵は装置そのものに永久に統合される要素によって必ずしも処理される必要がないことを理解すべきである。

【００５０】

特に、好ましい実施形態では、レコーダおよび／またはデコーダ装置は、この装置に関連し、前述の暗号化ステップあるいは暗号解読ステップのいくつかあるいは全てを実行するために使用される携帯セキュリティモジュールをさらに含む。

【００５１】

このような携帯セキュリティ装置は、デコーダあるいはレコーダの物理的サイ

ズおよび特性に応じて任意の便宜的な形をとることができる。例えば、スマートカードあるいはＰＣＭＣＩＡ型式カードは、デコーダと併用されてもよいし、ＳＩＭカードあるいは類似のカードはレコーダと併用されてもよい。

【００５２】

本発明の特定の好ましい実施形態では、第１の装置はレコーダ装置に対応し、第２の装置はデコーダ装置に対応する。このようなシステムでは、デコーダシステムマネージャは、例えば、レコーダメーカーに出される証明証の生成に対する最終制御を有する。同様な通信はレコーダによって開始され、レコーダが正しいシステム証明証および／または管理証明証を通信した場合、デコーダは、両方向通信を生じさせるように必要とされる情報を含む暗号化メッセージだけを通信する。

【００５３】

デコーダおよびレコーダが物理的に分離される場合、本発明は特に便利であるが、本発明は、例えば、組合せ装置内のレコーダ装置とデコーダ装置との間に安全なバスリンクを提供するように組合せのレコーダ装置／デコーダ装置で同様に使用されてもよい。

【００５４】

本発明は、デコーダがディジタルテレビジョン伝送を受信するように構成されるディジタルテレビジョン伝送システムと併用するために特に構成されるが、排他的に構成されていない。

【００５５】

本発明は、通信の方法に関して上記に記載された。本発明は、同様にこのような方法で使用するために構成された第１および第２の装置およびこのようなシステムで使用するために構成された１つあるいはそれ以上の携帯セキュリティモジュールに及ぶ。

【００５６】

私用／公開鍵を生成するための本発明で使用するのに適しているアルゴリズムは、例えば、ＲＳＡあるいはディフィ－ヘルマンを含んでもよく、適当な対称鍵アルゴリズムは、例えばＤＥＳ形式アルゴリズムを含んでもよい。しかしながら

、状況からみて必須でない限りあるいは別段の指定がない限り、対称アルゴリズムに関連した鍵と公開／私用アルゴリズムに関連した鍵との一般的な区別は全然行われない。

【００５７】

用語「スクランブル」および「暗号化」および「制御ワード」および「鍵」は、用語を明瞭にする目的のために本文のいろいろの部分で使用された。しかしながら、「スクランブルデータ」と「暗号化データ」との基本的な区別あるいは「制御ワード」と「鍵」との基本的な区別が全然行われるべきでない。同様に、用語「等しい鍵」は、最初に述べた鍵によって暗号化されるデータを暗号解読するように構成される鍵、またその逆に構成される鍵を示すために使用される。

【００５８】

ここで使用されるような用語「受信機／デコーダ」あるいは「デコーダ」は、符号化信号あるいは非符号化信号のいずれか、例えば、いくつかの他の手段によって放送あるいは伝送されてもよいテレビジョン信号および／またはラジオ信号を受信する受信機を含んでもよい。前記用語は、また受信信号を復号化する為のデコーダを含む。このようなデコーダの実施形態は、受信信号を復号化する受信機と一体のデコーダ、例えば、「セットトップボックス」において、物理的に別個の受信機と組合せて作動するデコーダ、あるいはウェブブラウザあるいはビデオレコーダあるいはテレビジョンのような付加的機能を含むこのようなデコーダも含んでもよい。

【００５９】

ここで使用されるように、用語「ディジタル伝送システム」は、例えば、主にオーディオビジュアルあるいはマルチメディアデータを伝送するかあるいは放送するいかなる伝送システムも含む。本発明は放送ディジタルテレビジョンシステムに特に応用可能であるが、本発明は、マルチメディアインターネット用途のための固定電気通信ネットワーク、閉回路テレビジョン等にも応用可能であってもよい。

【００６０】

ここで使用されるように、用語「ディジタルテレビジョンシステム」は、例え

ば任意の衛星、地上、ケーブルおよび他のシステムを含む。

【００６１】

次に、下記の図を参照して多数の本発明の実施形態だけを例として説明される。

【００６２】

ディジタルテレビジョン放送および受信システム１の概要が図１に示されている。本発明は、圧縮ディジタル信号を伝送するためにＭＰＥＧ－２圧縮システムを使用する大部分の従来ディジタルテレビジョンシステム２を含んでいる。より詳細には、放送センターのＭＰＥＧ－２圧縮器３はディジタル信号ストリーム（例えば、オーディオあるいはビデオ信号のストリーム）を受信する。圧縮器３は、リンク装置５によってマルチプレクサ・スクランブラ４に接続されている。マルチプレクサ４は、複数の他の入力信号を受信し、１つあるいはそれ以上のトランスポートストリームを組み立て、もちろん通信リンクを含むいろいろの形式をとることができるリンク装置７を介して圧縮ディジタル信号を放送センターの送信機６に送信する。

【００６３】

送信機６は、電磁信号が電子的に処理され、概念的なダウンリンク１０を介して従来はエンドユーザによって所有されるかあるいは賃貸されるディッシュアンテナの形の地上受信機１１に放送される衛星トランスポンダ９の方へ電磁信号をアップリンク８を介して送信する。受信機１１によって受信された信号は、エンドユーザによって所有されるかあるいは賃貸され、エンドユーザのテレビセット１３に接続される統合受信機／デコーダ１２に送信される。受信機／デコーダ１２は、圧縮ＭＰＥＧ－２信号をテレビセット１３のためのテレビジョン信号に復号化する。

【００６４】

条件付アクセスシステム２０は、マルチプレクサ４および受信機／デコーダ１２に接続され、一部は放送センターにあり、一部はデコーダにある。それによって、エンドユーザは、１つあるいはそれ以上の放送サプライヤーからのディジタルテレビジョン放送をアクセスできる。コマーシャル提供（すなわち、放送サプ

ライヤーによって販売された１つあるいはいくつかのテレビジョンプログラム）に関連するメッセージを暗号解読できるスマートカードは受信機／デコーダ１２に挿入できる。デコーダ１２およびスマートカードを使用して、エンドユーザは、加入モードあるいはペイ・パー・ビューモードのいずれかでイベントを購入してもよい。

【００６５】

マルチプレクサ４および受信機／デコーダ１２にも接続され、さらに一部は放送センターにあり、一部はデコーダにある対話システム１７は、エンドユーザがモデムバックチャネル１６を介していろいろのアプリケーションと対話できるように備えられてもよい。

【００６６】

次に、条件付アクセスシステム２０はより詳細に説明される。図２を参照すると、概要において、条件付アクセスシステム２０は、加入者許可システム（ＳＡＳ）２１を含む。ＳＡＳ２１は、例えば、それぞれのＴＣＰ－ＩＰリンク装置２３によって各々が各放送サプライヤーのための１つあるいはそれ以上の加入者管理システム（ＳＭＳ）２２に接続される（他の種類のリンク装置がその代わりに使用できるけれども）。それとは別に、１つのＳＭＳは、２つの放送サプライヤー間で共有でき、また１つのサプライヤーは２つのＳＭＳ等を使用できる。

【００６７】

「マザー」スマートカード２５を使用する演算装置２４の形の第１の暗号化装置は、リンク装置２６によって接続されている。さらに、マザースマートカード２８を使用する演算装置２７の形の第２の暗号化装置は、リンク装置２９によってマルチプレクサ４に接続されている。受信機／デコーダ１２は、例えば、「ドーター」スマートカード３０の形の携帯セキュリティモジュールを収容する。この受信機／デコーダ１２は、モデムバックチャネル１６を介して通信サーバ３１によってＳＡＳ２１に直接接続される。ＳＡＳは、特に加入権を要求に応じてドータースマートカードに送信する。

【００６８】

スマートカードは１人あるいはそれ以上の商業上のオペレータの秘密を含む。

「マザー」スマートカードは異なる種類のメッセージを暗号化し、「ドーター」スマートカードは、暗号解読する権利を有する場合、このメッセージを暗号解読する。

【００６９】

第１および第２の演算装置２４および２７は、ラックと、ＥＥＰＲＯＭに記憶されたソフトウェアを有する電子ＶＭＥカードと、最高２０枚の電子カードと、各電子カードのための１枚のスマートカード２５および２８とをそれぞれ備え、１枚のカード２８はＥＣＭを暗号化するためのものであり、１枚のカード２５はＥＭＭを暗号化するためのものである。

【００７０】

次に、ディジタルテレビジョンシステムの条件付アクセスシステム２０の動作は、テレビジョンシステム２および条件付アクセスシステム２０のいろいろの構成要素を参照してより詳細に説明される。

【００７１】

（マルチプレクサおよびスクランブラ）

図１および図２を参照すると、放送センターでは、ディジタルオーディオあるいはビデオ信号は、ＭＰＥＧ－２圧縮器３を使用して最初に圧縮される（あるいはビットレート減少される）。次に、この圧縮信号は、他の圧縮データのような他のデータと多重化されるためにリンク装置５を介してマルチプレクサ・スクランブラ４に伝送される。

【００７２】

このスクランブラは、スクランブル処理で使用され、マルチプレクサでＭＰＥＧ－２ストリームに含められる制御ワードを生成する。制御ワードは、内部で生成され、この制御ワードによって、エンドユーザの統合受信機／デコーダ１２はプログラムをデスクランブルできる。

【００７３】

いかにプログラムが商品化されるかを示すアクセス基準はＭＰＥＧ－２にも付加される。このプログラムは、多数の「加入」モードの中の１つおよび／または多数の「ペイ・パー・ビュー」（ＰＰＶ）モードの中の１つのいずれかで商品化

されてもよい。加入モードでは、エンドユーザは、１つあるいはそれ以上のコマーシャル提供、あるいは「ブーケ（ｂｏｕｑｕｅｔ）」に加入する、したがってこれらのブーケ内部のあらゆるチャネルを見る権利を得る。好ましい実施形態では、最高９６０のコマーシャル提供はチャネルのブーケから選択されてもよい。

【００７４】

ペイ・パー・ビューモードでは、エンドユーザは、望むようなイベントを購入する能力を備えられている。これは、前以てイベントをプレブッキングするか（プレブックモード）あるいはイベントが放送されるや否や事象を購入する（「インパルスモード」）のいずれかによって得ることができる。好ましい実施形態では、全てのユーザは加入モードあるいはＰＰＶモードで見ても見なくても、全てのユーザは加入者であるが、もちろんＰＰＶ視聴者は必ずしも加入者である必要がない。

【００７５】

（権利付与制御メッセージ）

制御ワードおよびアクセス基準の両方は、権利付与制御メッセージ（ＥＣＭ）を形成するために使用される。これは、スクランブルプログラムに関して送信されたメッセージである。すなわち、このメッセージは、放送プログラムの制御ワード（プログラムのデスクランブルを可能にする）およびアクセス基準を含む。アクセス基準および制御ワードは、リンク装置２９を介して第２の暗号化装置２７に伝送される。この装置では、ＥＣＭは、生成され、暗号化され、マルチプレクサ・スクランブラ４上に伝送される。放送伝送中、制御ワードは、一般的には２、３秒毎に変わるので、ＥＣＭも、変更制御ワードがデスクランブルできるように周期的に伝送される。冗長性目的のために、各ＥＣＭは、一般的には２つの制御ワード、すなわち現制御ワードおよび次制御ワードを含む。

【００７６】

データストリームで放送サプライヤーによって放送される各サービスは、多数の別個の構成要素を含む。すなわち、例えば、テレビジョンプログラムは、ビデオ構成要素、オーディオ構成要素、サブタイトル構成要素等を含む。サービスのこれらの構成要素の各々は、トランスポンダ９へのその後の放送のために個別に

スクランブルされ、暗号化される。サービスの各スクランブル構成要素に関しては、別個のＥＣＭが必要とされる。それとは別に、単一ＥＣＭは、サービスのスクランブル構成要素の全てに対して必要とされてもよい。複数のＥＣＭは、複数の条件付アクセスシステムが同じ伝送プログラムへのアクセスを制御する場合にも生成される。

【００７７】

（権利付与管理メッセージ（ＥＭＭ）

ＥＭＭは、個別エンドユーザ（加入者）、あるいはエンドユーザのグループに専用のメッセージである。各グループは所与の数のエンドユーザを含んでもよい。グループとしてのこの構成はバンド幅を最適化することに向けている。すなわち、１グループへのアクセスは多数のエンドユーザの獲得を可能にすることができる。

【００７８】

様々な特定の種類のＥＭＭを使用できる。個別のＥＭＭは個別の加入者の専用であり、一般的にはペイ・パー・ビューサービスの手段で使用される。すなわち、これらは、このグループの加入者のグループ識別子およびポジションを含む。

【００７９】

グループ加入ＥＭＭは、例えば２５６の個別のユーザのグループの専用であり、一般的にはいくつかの加入サービスの管理で使用される。このＥＭＭは、グループ識別子および加入者のグループビットマップを有する。

【００８０】

視聴者ＥＭＭは、全視聴者の専用であり、例えば、所定の自由サービスを行うために特定のオペレータによって使用されてもよい。「視聴者」は、同じ条件付アクセスシステム識別子（ＣＡ　ＩＤ）を持つスマートカードを有する加入者全体である。最後に、「独自の」ＥＭＭはスマートカードの独自の識別子にアドレス指定される。

【００８１】

ＥＭＭは、上記に概略されたようにオペレータによって伝送されたプログラムに関連した権利へのアクセスを制御するためにいろいろのオペレータによって生

成されてもよい。ＥＭＭは、一般に条件付アクセスシステムの態様を構成するように条件付アクセスシステムマネージャによっても生成されてもよい。

【００８２】

（プログラム伝送）

マルチプレクサ４は、ＳＡＳ２１からの暗号化ＥＭＭと、第２の暗号化装置２７からの暗号化ＥＣＭと、圧縮器３からの圧縮プログラムとを含む電気信号を受信する。マルチプレクサ４は、プログラムをスクランブルし、スクランブルプログラム、暗号化ＥＭＭおよび暗号化ＥＣＭをリンク装置７を介して放送センターの送信機６に送信する。送信機６は、アップリンク８を介して衛星トランスポンダ９の方へ電磁信号を送信する。

【００８３】

（プログラム受信）

衛星トランスポンダ９は、送信機６によって送信される電磁信号を受信し、処理し、この信号を、従来はエンドユーザによって所有されるかあるいは賃貸されるディッシュアンテナの形の地上受信機１１上にダウンリンク１０を介して送信する。受信機１１によって受信された信号は、エンドユーザによって所有されるかあるいは賃貸され、エンドユーザのテレビ受像機セット１３に接続される統合受信機／デコーダ１２に送信される。受信機／デコーダ１２は、この信号を多重分離し、暗号化ＥＭＭおよび暗号化ＥＣＭを有するスクランブルプログラムを得る。

【００８４】

プログラムがスクランブルされない場合、すなわち、ＥＣＭがＭＰＥＧ－２ストリームとともに全然送信されない場合、受信機／デコーダ１２は、データを伸長し、この信号をテレビ受像機セット１３に送信するためのビデオ信号に変換する。

【００８５】

プログラムがスクランブルされる場合、受信機／デコーダ１２は、対応するＥＣＭをＭＰＥＧ－２ストリームから抽出し、ＥＣＭをエンドユーザの「ドーター」スマートカード３０に送る。これは、受信機／デコーダ１２のハウジングにう

まくはまる。ドータースマートカード３０は、エンドユーザがＥＣＭを暗号解読し、プログラムをアクセスする権利を有するかどうかを制御する。有していない場合、否定状態が、プログラムをデスクランブルできないことを示すように受信機／デコーダ１２に送られる。エンドユーザがこの権利を有する場合、ＥＣＭが、暗号解読され、制御ワードが抽出される。次に、デコーダ１２は、この制御ワードを使用してプログラムをデスクランブルできる。ＭＰＥＧ－２ストリームは、伸長され、テレビ受像機セット１３へ前方伝送するためのビデオ信号に変換される。

【００８６】

（加入者管理システム（ＳＭＳ））

加入者管理システム（ＳＭＳ）２２は、特にエンドユーザファイル、コマーシャル提供、加入、ＰＰＶ詳細、およびエンドユーザ消費額および許可に関するデータの全てを管理するデータベース３２を含む。ＳＭＳは物理的にＳＡＳから離れてもよい。

【００８７】

各ＳＭＳ２２は、エンドユーザに送信される権利付与管理メッセージ（ＥＭＭ）の修正あるいは作成を意味するメッセージをそれぞれのリンク装置２３を介してＳＡＳ２１に送信する。

【００８８】

ＳＭＳ２２は、ＥＭＭの修正あるいは作成を意味しなくて、エンドユーザの状態の変化だけを意味するメッセージ（製品を注文する場合、エンドユーザに付与された許可あるいはエンドユーザが請求される金額に関する）をＳＡＳ２１にも送信する。

【００８９】

ＳＡＳ２１は、メッセージ（一般的には、コールバック情報あるいは課金情報のような情報を要求する）をＳＭＳ２２に送信するので、２つの間の通信は双方向であることが明らかである。

【００９０】

（加入者許可システム（ＳＡＳ））

ＳＭＳ２２によって生成されたメッセージは、リンク装置２３を介して加入者許可システム（ＳＡＳ）２１に送られる。この加入者許可システム（ＳＡＳ）２１は、同様にＳＭＳ２１によって生成されたメッセージの受信を肯定応答するメッセージを生成し、これらの肯定応答をＳＭＳ２２に送る。

【００９１】

概要において、ＳＡＳは、加入モードのための権利を与え、毎月この権利を自動的に更新する加入チェーン領域と、ＰＰＶイベントのための権利を与えるペイ・パー・ビューチェーン領域と、加入チェーン領域およびＰＰＶチェーン領域によって作成されたＥＭＭをマルチプレクサ・スクランブラ４に送り、この故にＥＭＭを有するＭＰＥＧストリームを供給するＥＭＭインジェクタとを含む。コンピュータソフトウェアをユーザのパーソナルコンピュータにダウンロードする場合のペイ・パー・ファイル（ＰＰＦ）権利のような他の権利が与えられるべきである場合、他の同様な領域も提供される。

【００９２】

ＳＡＳ２１の１つの機能は、加入モードでコマーシャル提供として利用可能であるかあるいは異なる商品化モード（プレブックモード、インパルスモード）によるＰＰＶイベントとして販売されるテレビジョンプログラムに対するアクセス権を管理することにある。これらの権利およびＳＭＳ２２から受信された情報によるＳＡＳ２１は加入者のためのＥＭＭを生成する。

【００９３】

ＥＭＭは、管理鍵および利用鍵に対して演算する演算装置（ＣＵ）２４に送られる。ＣＵは、ＥＭＭのシグネチャを完了し、ヘッダが付加される、ＳＡＳ２１のメッセージ生成器（ＭＧ）にＥＭＭを送り返す。ＥＭＭは、完全ＥＭＭとしてメッセージ放出器（ＭＥ）に送られる。メッセージ生成器は、放送開始・終了時間およびＥＭＭの放出速度を決定し、これらをＥＭＭとともに適切な指令に応じてメッセージ放出器に送る。このＭＧは所与のＥＭＭを一度生成するだけである。すなわち、ＥＭＭの周期的伝送を実行するのはＭＥである。

【００９４】

ＥＭＭを生成する際に、ＭＧは独自の識別子をＥＭＭに割り当てる。ＭＧがＥ

ＭＭをＭＥに送る場合、ＥＭＭ　ＩＤもまた送る。このことが、ＭＧおよびＭＥの両方にて特定のＥＭＭの識別を可能にする。

【００９５】

複数の動作に関連した複数の条件付アクセスシステム等を扱うのに適しているシステムにおいて、各条件付アクセスシステムに関連したＥＭＭストリームは、別々に生成され、伝送前にマルチプレクサ４によって一緒に多重化される。

【００９６】

（放送システムの暗号化レベル）

次に図３を参照すると、標準放送システムの暗号化レベルの簡略大要が今説明される。ディジタルデータの放送に関連した暗号化段が４１に示され、伝送チャネル（例えば前述のような衛星リンク）が４２に示され、受信機の暗号解読段が４３に示される。

【００９７】

ディジタルデータＮは、その後の伝送のためにマルチプレクサＭｐに伝送される前に制御ワードＣＷによってスクランブルされる。図３の下部から分かるように、伝送データは、とりわけ、利用鍵Ｋｅｘによって制御される暗号器Ｃｈ１によって暗号化されるような制御ワードＣＷを含むＥＣＭを含んでいる。受信機／デコーダで、この信号は、見るためにテレビ１３に送られる前にデマルチプレクサＤＭｐおよびデスクランブラＤによって送る。鍵Ｋｅｘも持つ暗号解読装置ＤＣｈ１は、多重分離信号のＥＣＭを暗号解読し、その後にこの信号をデスクランブルするために使用される制御ワードＣＷを得る。

【００９８】

セキュリティ理由のために、暗号化ＥＣＭに埋め込まれた制御ワードＣＷは、平均で１０秒等毎に変わる。ＥＣＭを復号化するために受信機によって使用される第１の暗号化鍵Ｋｅｘは、毎月変更されるかあるいは演算子ＥＭＭによって変更される。暗号化鍵Ｋｅｘは、個人の専用とされるグループ鍵Ｋ１（ＧＮ）を使用して第２の装置ＣｈＰによって暗号化される。加入者が更新鍵Ｋｅｘを受信するように選択された加入者の中の１人である場合、デコーダセキュリティモジュールの暗号解読装置ＤＣｈＰは、そのグループ鍵Ｋ１（ＧＮ）を使用してこのメ

ッセージを暗号解読し、その月の鍵Ｋｅｘを得る。

【００９９】

暗号解読装置ＤＣｈｐおよびＤＣｈ１ならびに関連鍵は、デコーダに関連したセキュリティモジュールに保有され、この場合、スマートカード３０は、加入者に供給され、デコーダのスマートカードリーダーに挿入される。この鍵は、例えば、任意の通常使用される対称鍵アルゴリズムあるいはカスタマイズされた対称鍵アルゴリズムに従って生成されてもよい。

【０１００】

前述されるように、異なる鍵は、異なるオペレータあるいは放送会社ならびに条件付アクセスシステムサプライヤーに関連してもよい。前記の説明では、グループ鍵Ｋ１（ＧＮ）は、デコーダに関連し、ＥＭＭメッセージを暗号解読するために使用されるスマートカードによって保有される。実際は、異なるオペレータは、異なる加入者の独自の鍵Ｋ１（Ｏｐ１，ＧＮ），Ｋ１（Ｏｐ２，ＧＮ）等を有する。各グループ鍵は、オペレータによって生成され、加入者が属するグループに関連した値によって多様化される。

【０１０１】

スマートカードの異なるメモリゾーンは異なるオペレータのための鍵を保有する。各オペレータは、当該のスマートカードにだけ関連する独自の鍵およびこのオペレータによって提供されたサービスの全ての加入者のための視聴者鍵も有してもよい（上記を参照）。

【０１０２】

さらに、鍵のセットは条件付アクセスシステムのマネージャによっても保有されてもよい。特に、所与のスマートカードは、全てのスマートカードに共通のユーザ専用鍵Ｋ０（ＮＳ）および視聴者鍵Ｋ１（Ｃ）を含んでもよい。オペレータ鍵は通常放送権に関連したＥＭＭメッセージを復号化するために使用されるが、条件付アクセスマネージャ鍵は、後述されるように、一般に条件付アクセスシステムの変更に関連したＥＭＭメッセージを暗号解読するために使用されてもよい。

【０１０３】

図３に示されたシステムの上記の説明は、伝送が単一デコーダによってデスクランブルされ、単一テレビディスプレイに表示される放送システムのアクセス制御の実行に関する。図４を参照すると、次に第１および第２のデコーダ構成が説明される。

【０１０４】

（デコーダ構成）

前述のように、デコーダ１２は、受信機１１を介してスクランブル放送伝送を受信する。このデコーダは、便宜的にはスマートカードの形をとってもよいが、任意の他の適当なメモリあるいはマイクロプロセッサ携帯装置を含んでもよい携帯セキュリティモジュール３０を含む。このデコーダ１２は、例えば、条件付アクセス情報を処理するサーバと通信するモデムチャネル１６に接続され、例えば、ペリテルリンク５３を介してデスクランブルオーディオビジュアルディスプレイ情報をテレビ１３に送るようにも構成される。

【０１０５】

このシステムは、例えばＩＥＥＥ１３９４バス５１を介してデコーダ１２と通信するように構成される従属あるいはスレーブデコーダ５０をさらに含む。このデコーダ５０は、スクランブル放送伝送を直接受信するために受信機１１あるいは他の衛星受信機に対する結線（図示せず）を含んでもよい。それとは別に、この情報は、結線５１を介して第１のデコーダ１２から送られてもよい。

【０１０６】

第２のデコーダ５０は、さらに携帯セキュリティモジュール５２で作動するように構成される。携帯セキュリティモジュール５２は、便宜的にはスマートカードとして実現されてもよい。しかしながら、ＰＣＭＣＩＡカード、マイクロプロセッサ鍵等のような従来公知であるような任意の携帯メモリおよび／またはマイクロプロセッサ装置が使用されてもよい。伝送をデスクランブルする際のこのモジュール５２の動作が後述される。

【０１０７】

このデコーダ５０は、デスクランブル伝送を表示するために使用されるテレビディスプレイ５５のリンク５４も含んでいる。デコーダ１２、５０およびディス

プレイ１３、５５の要素は別々に示されているが、これらの要素のいくつかあるいは全ては例えば、組合せデコーダ／テレビセットを提供するように合体されてもよいことを思い描いている。

【０１０８】

（デコーダ間の安全な通信）

序論で述べられているように、加入データの管理に関する問題を避けるために、単一加入だけが２つのデコーダ１２、５０の所有者のために開かれていることが望ましい。デコーダ１２はシステムの主デコーダあるいは第１のデコーダである場合、スマートカード３０は、図３に関して前述されたような毎月の利用鍵Ｋｅｘを受信するように個人の専用とされる。デコーダ５０が伝送をデスクランブルし、ディスプレイ５５を介して表示できるために、このデスクランブルが実行できるように所定の情報をセキュリティモジュール３０からセキュリティモジュール５２に通信することが必要である。

【０１０９】

本実施形態では、スマートカード３０は、制御ワードＣＷ値を得るために伝送に関連したＥＣＭメッセージを暗号解読する。次に、この制御ワード値が、伝送をデスクランブルし、ディスプレイ５５を介してプログラムを表示するためにデコーダ５０およびスマートカード５２によって使用される場合、暗号化形式でリンク５１を介してデコーダ５０およびスマートカード５２に通信される。

【０１１０】

それにもかかわらず、例えば、毎月の利用鍵Ｋｅｘのコピーはデコーダおよびスマートカード５０、５２に送られ、デコーダ５０がその後に独立して作動できる、この制御ワード実施形態以外の実施形態を思い描いてもよい。

【０１１１】

理解されているように、いかなる詐欺の問題も回避するために、制御ワード情報あるいは実際に伝送を暗号解読し、デスクランブルする際に使用される少しの他の情報も決して暗号化されていない形式でリンク５１を介して伝送されないことがきわめて重要である。

【０１１２】

次に、このような通信リンクが実現できる方法が図５および図６を参照して説明される。

【０１１３】

明瞭にするために、公開／私用鍵アルゴリズムを使用する全ての暗号化動作は記号ｆａによって示されるのに対して、対称アルゴリズムを使用する全ての動作は記号ｆｓによって示される。暗号解読動作は「ｆａあるいはｆｓ」として示される。

【０１１４】

私用／公開鍵対は、ＲＳＡあるいはディフィ－ヘルマンのような任意の適当な非対称暗号化アルゴリズムに従って生成されてもよい。対称鍵はＤＥＳのようなアルゴリズムと併用されてもよい。いくつかの場合、カスタム対称アルゴリズムも使用されてもよい。

【０１１５】

図５を参照すると、デコーダ５０のためのスマートカード５２は、６５に示され、６１に示された私用管理鍵ＫｐｒｉＭａｎに関連した公開鍵と同等の公開鍵ＫｐｕｂＭａｎで個人の専用とされる。実際には、従属あるいはスレーブデコーダと併用されることを意図される全てのスマートカード５２は、鍵ＫｐｕｂＭａｎを含む。

【０１１６】

この個人専用化ステップは、カードの最初の個人専用化の瞬間（第２のデコーダを提供することを既に思い描いている場合）あるいはユーザが加入の際に第２のデコーダを含めることを要求する場合のいずれかでシステムマネージャの本部で通常内密に実行される。

【０１１７】

その後、６１に示された秘密私用鍵ＫｐｒｉＭａｎを持つシステムマネージャは、専用ＥＭＭメッセージ６２で６３に示された証明証Ｃｔ（ＫｐｕｂＴ）を通信する。証明証は、公開鍵ＫｐｕｂＴを私用マネージャ鍵ＫｐｒｉＭａｎで暗号化することによって作成される。ＥＭＭは、６４に示され、スマートカード３０の不揮発性メモリに証明証Ｃｔ（ＫｐｕｂＴ）とともに記憶された私用鍵Ｋｐｒ

ｉＴをさらに含む。

【０１１８】

デコーダ１２およびカード３０のみこのＥＭＭメッセージを暗号解読してもよいので、ＥＭＭそのものは、適切な伝送あるいは利用鍵を使用して１つのデコーダの専用のＥＭＭのために通常の方法で暗号化される。

【０１１９】

２つのデコーダがＩＥＥＥ１３９４リンク５１を介して通信状態にする瞬間に、スマートカード３０は、６６に示されるように証明証Ｃｔ（ＫｐｕｂＴ）をスマートカード５２に送信する。公開鍵ＫｐｕｂＭａｎを使用すると、カードは、６８で示されるような公開鍵ＫｐｕｂＴを得るために６７の証明証を暗号解読する。この公開鍵ＫｐｕｂＴは、その後、デコーダ対１２、５０およびカード対３０、５２に特に関連している。

【０１２０】

このカード５２は、その後、６９に示されるランダム鍵値Ｋｓを生成する。記載されているように、このランダム鍵は、後で、カード３０、５２間で両方向に通信されるメッセージを暗号化するために対称アルゴリズムでセッション鍵として使用される。新しいセッション鍵値は、システムのデコーダ５０およびカード５２のその後の再接続毎に生成されてもよい。すなわち、毎回デコーダ５０は、ユーザによって、あるいは例えばペイ・パー・ビューフィルムの視聴セッション毎にオンにスイッチされる。

【０１２１】

対称鍵Ｋｓは、７１でスマートカード３０に送信された公開鍵ＫｐｕｂＴおよび暗号化値を使用して７０で暗号化される。このカード３０は、７３で私用鍵ＫｐｒｉＴによってメッセージを暗号解読し、７２でセッション鍵値を記憶する。理解されるように、私用／公開暗号化アルゴリズムの特性のために、暗号化メッセージは、私用鍵ＫｐｒｉＴを持つカード、すなわちカード３０によってのみ暗号解読されてもよい。

【０１２２】

前述のように、カード３０、５２は、値ＫｐｒｉＴ、Ｃｔ（ＫｐｕｂＴ）およ

びＫｐｕｂＭａｎをそれぞれのカード３０、５０に埋め込むかあるいは通信する同じシステムマネージャによってプログラム化される。他の具現（図示せず）では、第２の許可層はシステム私用鍵ＫｐｒｉＳｙｓｔｅｍを使用して提供されてもよい。この具現では、ＫｐｒｉＳｙｓｔｅｍによって暗号化された鍵ＫｐｕｂＭａｎを含む証明証Ｃｔ（ＫｐｕｂＭａｎ）はカード３０に記憶される。

【０１２３】

このような具現では、カード５２はさらに二次システム公開鍵ＫｐｒｉＳｙｓｔｅｍを持つ。動作の際に、カード３０は、証明証Ｃｔ（ＫｐｕｂＭａｎ）の暗号化値をＫｐｒｉＳｙｓｔｅｍを使用してこのメッセージを暗号解読し、ＫｐｕｂＭａｎを得るカード５２に送信する。それ以来、このステップは前述と同じであり、カード５２はＫｐｕｂＴ等を得るために鍵ＫｐｕｂＭａｎを使用する。

【０１２４】

次に、図６を参照すると、カード３０からカード５２への制御ワード情報の安全な通信に必要されるステップが今説明される。

【０１２５】

通常の動作の際、スレーブデコーダ５０およびカード５２は、伝送をデスクランブルするのに必要な制御ワード情報を含む暗号化ＥＣＭメッセージとともにスクランブル伝送を受信する。これらのＥＣＭメッセージは、７５でＩＥＥＥ１３９４を介してマスタデコーダおよびカード１２、３０に送られる。それとは別に、スレーブデコーダを介して表示される伝送のためのＥＣＭメッセージは、マスタデコーダおよびカード１２、３０によって直接受信されてもよい。

【０１２６】

次に、カード３０は、標準検証ステップを７６で実行し、デコーダの１つあるいは両方がこの伝送をアクセスする権利を有することをチェックする。デコーダが必要な権利を有しない場合、「無効」メッセージ７７はデコーダおよびカード５０、５２に戻され、この処理は停止する。

【０１２７】

加入者が必要な権利を持っていると仮定すると、７９に示され、暗号化制御ワードＣＷを含むＥＣＭメッセージは、そのとき、システムマネージャあるいはオ

ペレータに関連した８１に示された毎月の利用鍵Ｋｅｘを使用して８０で暗号解読される。

【０１２８】

８１に示された制御ワードの暗号化されていない値は、そのとき、８３に示された予め得られたセッション鍵Ｋｓを使用して８２で再暗号化される。理解されるように、制御ワードの再暗号化のための８２で使用された暗号化アルゴリズムは、８０で使用された暗号化アルゴリズムに相当し、実際に、セキュリティ理由のために、異なるアルゴリズムが使用されてもよい。便宜的には、システムマネージャ所有のカスタムアルゴリズムは、８０に示された暗号解読ステップおよび８０に示されたセッションメッセージの暗号化のために使用されたＤＥＳのような一般的なアルゴリズムを含む利用鍵Ｋｅｘに関するステップのために使用されてもよい。

【０１２９】

いくつかの場合、著作権告示情報のような付加情報は、制御ワードＣＷおよびこの付加情報がＫｓによって暗号化され、第２のデコーダおよびカードに送信されるようにステップ８１および８２間に導入されてもよい。このような情報の存在は、第２のデコーダがデータを記録するかあるいはこの情報をレコーダに送ることができる場合により重要である。著作権告示は、第２のデコーダがデータを記録するかあるいは例えば無限回数データを記録および再生することを防止するためにフラグとして使用されてもよい。

【０１３０】

暗号化制御ワードは、８３に示されるようにデコーダ５０およびカード５２に戻される。８４に示された等しいセッション鍵Ｋｓを使用すると、このカードは、８５でメッセージを暗号解読し、８６に示された暗号化されていない制御ワードを得る。その後、この制御ワード値は、関連テレビディスプレイ５５にその後表示するために伝送の関連部をデスクランブルするためにデコーダおよびカード５０、５２によって使用される。

【０１３１】

いくつかの場合、デコーダ５０およびカード５２がＶＣＲのような他のオーデ

ィオビジュアル装置に情報を送ることを望んでもよいことを思い描いてもよい。このような例では、デコーダ５０およびカード５２には、「マスタ」装置の役割を引き受けるのに必要な私用鍵が供給されてもよく、同じ動作が、必要に応じて変更を加えて安全なリンクを生じさせるようにデコーダと他の装置との間で実行されてもよい。

【０１３２】

上記の説明は一対のデコーダに関する情報の確認および通信に焦点を合わせているが、本発明は、同様に一連の相互接続デコーダ、例えば、各々が等しい公開鍵ＫｐｕｂＴを持つ複数の従属デコーダからのメッセージの暗号解読のための複数の私用トランスポート鍵ＫｐｒｉＴを持つ単一マスタデコーダを保護するように拡張されてもよい。

【０１３３】

さらに、デコーダからレコーダへ通信されるデータは前述の例では制御ワードを含むが、伝送をデスクランブルすることに直接関連しない情報さえ含む他の情報はこのリンクを介して送られてもよい。

【０１３４】

同様に、上記に述べられたのと同じ原理は、ディジタルＶＣＲ、ディジタルテレビあるいはこのような装置の任意の組合せのようなネットワークに接続された他のディジタルオーディオビジュアル装置間の通信に適用されてもよい。例えば、図７を参照すると、スクランブル伝送の記録および再生のためのアクセス制御システムの要素が、次に説明される。

【０１３５】

（デコーダおよびレコーダ構成）

前述のように、デコーダ１２は、受信機１１を介してスクランブル放送伝送を受信する。このデコーダは、便宜的にはスマートカードの形をとるが、任意の他の適当なメモリあるいはマイクロプロセッサ装置を含んでもよい携帯セキュリティモジュール３０を含む。デコーダ１２は、例えば、条件付アクセス情報を処理するサーバと通信するモデムチャネル１６を含み、デスクランブルオーディオビジュアルディスプレイ情報を、例えばペリテルリンク５３を介してテレビ１３に

も送るように構成されている。このシステムはさらに、例えばＩＥＥＥ１３９４バス１０１を介してデコーダと通信するように構成されるＤＶＨＳあるいはＤＶＤレコーダのようなディジタルレコーダ１００を含む。レコーダ１００は、情報が記録されるディジタル記録支持体（図示せず）を収容する。

【０１３６】

レコーダ１００はさらに、とりわけ、記録の再生へのアクセスを制御するために使用される鍵を含む携帯セキュリティモジュール１０２で作動するように構成されている。携帯セキュリティモジュールは、従来公知であるような例えばスマートカード、ＰＣＭＣＩＡカード、マイクロプロセッサ鍵等の任意の携帯メモリおよび／またはマイクロプロセッサ装置を含んでもよい。この場合、携帯セキュリティモジュール１０２は、携帯電話の分野で公知であるようなＳＩＭカードとして示されている。

【０１３７】

ディジタルレコーダ１００は、ディスプレイ１３への直接リンク１０４を含む。他の具現では、ディジタルオーディオビジュアル情報は、表示前レコーダ１００からデコーダ１２へ送られてもよい。同様に、デコーダ１２、レコーダ１００およびディスプレイ１３の要素は別々に示されているが、これらの要素のいくつかあるいは全ては、例えば、組合せデコーダ／テレビセットあるいは組合せデコーダ／レコーダ等を提供するように合体されてもよいことが考えられる。

【０１３８】

同様に、本発明はオーディオビジュアル放送情報の記録に関して検討されているが、本発明も、便宜的には、例えば、ＤＡＴあるいはミニディスクレコーダにその後記録された放送排他オーディオ情報あるいはコンピュータのハードディスクに記録された放送ソフトウェアアプリケーションにさえ適用されてもよい。

【０１３９】

（デコーダとレコーダとの間の安全な通信）

序論に述べられているように、記録鍵でのスクランブル伝送と関連する制御ワードを再暗号化し、スクランブル伝送とともに再暗号化制御ワードを記録支持体に記憶することは従来の提案されたシステムから公知である。最初の伝送の暗号

化および暗号解読に関連した利用鍵と違って、記録鍵は、記録が将来いつでも再生できるようにこの特定の記録に関連した変更しない鍵であってもよい。

【０１４０】

図７の概要から分かるように、デコーダ要素からのシステムの記録要素の独立を可能にするために、記録鍵が、例えば、携帯セキュリティモジュールＳＩＭカード１０２のようなレコーダに関連したセキュリティモジュールに鍵を記憶することによってレコーダ１００と関連すべきであることが必要である。特に、鍵がデコーダ１２あるいはスマートカード３０に永久に記憶される場合、レコーダは、デコーダがない場合、記録を再生できない。

【０１４１】

これを行うために、リンク１０１に沿ってデコーダ１２とレコーダ１００との間に所定の情報を送る必要がある。この情報は、例えば、次にディジタルレコーダで記録鍵の使用によって再暗号化されてもよい制御ワード情報を暗号解読されてもよい。それとは別に、制御ワード情報はデコーダによって生成された記録鍵によって暗号化されてもよく、この記録鍵はそのとき記憶するためのレコーダに送信される。

【０１４２】

全ての場合、デコーダとレコーダとの間で安全化リンクを確実することは必要である。あいにく、デコーダの働きをする放送システムマネージャとレコーダの働きをするレコーダ装置のメーカーとの間の活動の独立は、この目的のための暗号化鍵の提供に関する多数の問題をもたらす。

【０１４３】

例えば、放送オペレータは、メーカーに例えば、レコーダセキュリティモジュール１０２によって必要とされる秘密対称アルゴリズム鍵を預け、デコーダセキュリティモジュール３０によって保有される等しい鍵を使用して暗号化された通信を暗号解読するようにレコーダの製造場所でセキュリティの保全性を十分な確信しなくてもよい。

【０１４４】

さらに、活動の分離によって、レコーダセキュリティモジュール１０２が適切

な鍵に関して個人の専用とするために放送システムマネージャに送信される状況を思い描くことは実用的でないこともある。この理由のために、デコーダおよびレコーダのための動作の最大独立を可能にする解決策を思い描くことが必要である。

【０１４５】

図８は、これらの問題を解決する、デコーダとレコーダセキュリティモジュール３０、１０２との間で安全な通信リンクを生じさせる方法を概略形式出示している。

【０１４６】

明瞭にするために、公開／私用鍵アルゴリズムを使用する全ての暗号化／暗号解読動作は六角形の記号ｆａによって示されるのに対して、対称アルゴリズムを使用する全ての動作は卵形の記号ｆｓによって示される。

【０１４７】

図５に示されるように、レコーダカード１０２は、放送システムマネージャによってレコーダメーカーに通信される１２０に示されるシステム証明証ＣｔＫｅｙＲｅｃを使用してレコーダメーカーによって作成される。１２１に示されるように、この証明証は、放送システム私用鍵ＫｐｒｉＳｙｓｔｅｍによって暗号化されたメーカー公開鍵ＫｐｕｂＭａｎに対応する。私用鍵ＫｐｒｉＳｙｓｔｅｍは、システムマネージャに固有であり、システムマネージャによって排他的に保有され、たとえ値ＫｐｕｂＭａｎが既知であるとしても、この鍵値を証明証ＣｔＫｅｙＲｅｃから得ることができない。

【０１４８】

下記からより明らかになるように、メーカー鍵ＫｐｕｂＭａｎを含むシステム証明証ＣｔＫｅｙＲｅｃは、メーカーの鍵システムのセキュリティの保全性、特に鍵ＫｐｕｂＭａｎの正当性の放送オペレータによる保証に役立つ。この証明証は１回だけ生成される。この証明動作において、メーカーは、鍵ＫｐｕｂＭａｎを私用鍵ＫｐｒｉＳｙｓｔｅｍを使用して鍵ＫｐｕｂＭａｎを暗号化し、システム証明証ＣｔＫｅｙＲｅｃを返す放送システムマネージャに通信する。その後、メーカーは、レコーダセキュリティモジュールの個人専用化ステップ中、証明証

ＣｔＫｅｙＲｅｃを含むように全レコーダセキュリティモジュールを構成する。

【０１４９】

鍵ＫｐｕｂＭａｎそのものは、レコーダメーカーあるいはレコーダの供給者のＩＤに関連し、レコーダメーカーあるいはレコーダの供給者に固有の私用／公開鍵対の公開鍵に対応する。対応する私用鍵ＫｐｒｉＭａｎは、排他的にはレコーダメーカーによって保有され、放送システムマネージャにさえ知られていない。鍵ＫｐｒｉＭａｎは、それ自体１２２に示された装置証明証ＣｔＫｅｙＳＩＭを生成するために使用される。レコーダセキュリティモジュールに固有であるこの証明証は、私用メーカー鍵ＫｐｒｉＭａｎによって暗号化されるレコーダセキュリティモジュール鍵ＫｐｕｂＳＩＭに対応する。

【０１５０】

鍵ＫｐｕｂＳＩＭは、同様にレコーダ装置のＩＤに関連し、このレコーダ装置に固有の私用／公開鍵対の公開鍵に対応する。この鍵および対応する私用鍵ＫｐｒｉＳＩＭはレコーダメーカーによって生成される。図示されるように、私用鍵ＫｐｒｉＳＩＭは、１２４で、好ましくはチップそのものの製造の瞬間にレコーダセキュリティモジュールに記憶される。

【０１５１】

暗号化通信が、デコーダと、例えば、デコーダによって受信された伝送の記録に関連したレコーダとの間で生じさせられるべきである場合、システム証明証ＣｔＫｅｙＲｅｃは、１２６に示されるようにレコーダセキュリティモジュール１０２からデコーダセキュリティモジュール３０に伝送される。

【０１５２】

デコーダセキュリティモジュール３０は、１２５に示され、放送システムマネージャによる個人専用化中にカード３０に記憶される放送システム公開鍵ＫｐｕｂＳｙｓｔｅｍを含む。システム鍵ＫｐｕｂＳｙｓｔｅｍを使用して、デコーダセキュリティモジュールは、メーカー公開鍵ＫｐｕｂＭａｎを得るために１２７で証明証ＣｔＫｅｙＲｅｃを暗号解読する。

【０１５３】

レコーダ供給者に関連したセキュリティ侵害の場合、セキュリティモジュール

３０は、暗号解読ステップ１２７後に得られた若干のメーカー公開鍵値を拒絶するようにプログラム化できる。特に、鍵ＫｐｕｂＭａｎは、１２８に記憶され、次の暗号解読ステップで使用される。

【０１５４】

１２９に示されるように、レコーダセキュリティモジュール１０２は、そのとき、このレコーダセキュリティモジュールに固有な装置証明証ＣｔＫｅｙＳＩＭをデコーダセキュリティモジュール３０に通信する。メーカー公開鍵ＫｐｕｂＭａｎを使用して、デコーダセキュリティモジュール３０は、レコーダセキュリティモジュール公開鍵ＫｐｕｂＳＩＭを１３０で暗号解読する。

【０１５５】

この公開鍵は、１３１でデコーダセキュリティモジュール３０に記憶され、次にセッション鍵値の暗号化および通信で使用される。この例では対称暗号化／暗号解読アルゴリズムによって使用可能な乱数値に対応するこのセッション鍵値は、１３２で生成され、レコーダセキュリティモジュール公開鍵ＫｐｕｂＳＩＭによって１３３で暗号化され、次に１３４でレコーダセキュリティモジュールに通信される。

【０１５６】

理解されるように、公開／私用鍵アルゴリズムの特性のために、この暗号化メッセージは、レコーダセキュリティモジュールに１２４で記憶される独自の私用鍵ＫｐｒｉＳＩＭを使用して暗号解読されるだけでよい。１３５でのメッセージの暗号解読は１３６でのセッション鍵の抽出をもたらす。

【０１５７】

その後、各セキュリティモジュール３０、１０２は、両方向メッセージの暗号化および暗号解読で使用するために１３７、１３８で対称セッション鍵のコピーを持つ。前述のように、セッション鍵は対称アルゴリズムと組合せて使用され、等しいセキュリティはいずれかの方向のメッセージのために提供される。両方向通信を必要としなくて非対称アルゴリズムを使用する他の実施形態を思い描いてもよい。

【０１５８】

図８に示されるように、セッション鍵は、本実施形態では、制御ワード情報をデコーダからレコーダへ通信するために使用される。特に、スクランブル伝送に関連したＥＣＭメッセージ１３９は、その中に含まれた任意の他の情報とともに制御ワード１４０の暗号化されていない値を得るためにデコーダセキュリティモジュールによって受信され、暗号解読される。次に、この制御ワードは、１３７で記憶されたセッション鍵を使用して１４１で再暗号化され、得られる暗号化メッセージは、１４２でレコーダセキュリティモジュール１０２に通信される。

【０１５９】

１３８で記憶されたセッション鍵を使用して、レコーダセキュリティモジュールは、１４３でメッセージを暗号解読し、１４４で制御ワードの暗号化されていない値を得る。次に、制御ワードは、レコーダセキュリティモジュールによって内部で生成され、１４６で記憶される記録鍵を使用して１４５で再暗号化される。この再暗号化制御ワードおよび任意の他の情報を含む新しいＥＣＭは、次に最初にスクランブル伝送とともに記録支持体１４７に記録される。記録の再生の際に、レコーダセキュリティモジュール１０２は、表示前にスクランブル伝送を暗号解読する際に使用される制御ワード値を得るようにＥＣＭを暗号解読するために１４６で記憶された記録鍵値を使用する。

【０１６０】

保護コピーを提供するために、記録鍵はセッション鍵を使用してデコーダに通信されてもよい。その後、この記録は、レコーダセキュリティモジュールの損傷あるいは損失の場合にバックアップとしてデコーダセキュリティモジュールに記憶される。

【０１６１】

私用／公開鍵対ＫｐｒｉＳＩＭ、ＫｐｕｂＳＩＭ、ＫｐｒｉＭａｎ、ＫｐｕｂＭａｎ、ＫｐｒｉＳｙｓｔｅｍおよびＫｐｕｂＳｙｓｔｅｍは、ＲＳＡあるいはディフィ－ヘルマンのような任意の適当な非対称暗号化アルゴリズムに従って生成されてもよい。同様に、セッション鍵および記録鍵は、ＤＥＳのような任意の適当な対称暗号化／暗号解読アルゴリズムとともに使用可能な鍵値に一致してもよい。

【０１６２】

理解されるように、上記の実施形態の代替の具現は可能である。この場合、例えば、同じシステムマネージャがデコーダセキュリティモジュールおよびレコーダセキュリティモジュールの両方を管理することを個人の専用とする責任を負っている場合、システム証明証ＣｔＫｅｙＲｅｃを使用する認証の最初のステップは、ＫｐｕｂＭａｎの値が１２８でデコーダモジュールに直接挿入されるので省略されてもよい。

【０１６３】

さらに、伝送送波および記録送波のセキュリティの保全性を保証する責任はレコーダのメーカーにある場合、デコーダセキュリティモジュールおよびレコーダセキュリティモジュールの役割のいくつかあるいは全ては、レコーダメーカーが放送システムオペレータによって提供される公開鍵を認証し、レコーダが通信の開始、セッション鍵の生成等の責任を負っているので、完全に逆にされてもよい。

【０１６４】

セッション鍵の生成のレベル以下で、記録で使用するための情報の通信に対する任意の数の可能性を思い描いてもよいことも分かる。例えば、デコーダからレコーダへ通信されるデータは前述された例では制御ワードを含むが、レコーダカードに通信する前にオーディオビジュアルデータそのものを暗号解読し、再暗号化することを思い描いてもよい。それとは別に、あるいはさらに、記録鍵は、デコーダセキュリティモジュールで生成され、レコーダセキュリティモジュールに通信されてもよい。

【０１６５】

さらに、前述の説明はレコーダあるいはデコーダの単一供給者に関する情報の確認および通信に焦点を合わせているが、本発明は同様に複数のデコーダ供給者および／またはレコーダ供給者を保護するように拡張してもよい。例えば、レコーダセキュリティモジュールは、複数の放送システムマネージャに関連した複数のシステム証明証ＣｔＫｅｙＲｅｃを含んでもよい。同様に、デコーダセキュリティモジュールは、第１の検証ステップが実行された後に得られる複数のレコー

ダメーカー管理鍵ＫｐｕｂＭａｎを処理するように構成されてもよい。

【０１６６】

変化するセッション鍵の使用はセキュリティのレベルを増加させるが、一定セッション鍵が使用されるかあるいは公開／私用鍵ＫｐｕｂＳＩＭ／ＫｐｒｉＳＩＭが一方の装置から他方の装置へ通信される情報を直接暗号化するために使用される場合、他の具現を思い描くことができる。セッション鍵そのものは私用／公開鍵対を含んでもよい。

【図面の簡単な説明】

【図１】

この実施形態によるディジタルＴＶシステムの全アーキテクチャを示している。

【図２】

図１の条件付アクセスシステムのアーキテクチャを示している。

【図３】

条件付アクセスシステムの暗号化レベルを示している。

【図４】

第１および第２のデコーダのレイアウトを示している。

【図５】

第１および第２のデコーダ間に安全な通信リンクを生じさせることに関連したステップを示している。

【図６】

安全な通信リンクを介して制御ワード情報を転送する際の第１および第２のデコーダの動作を示している。

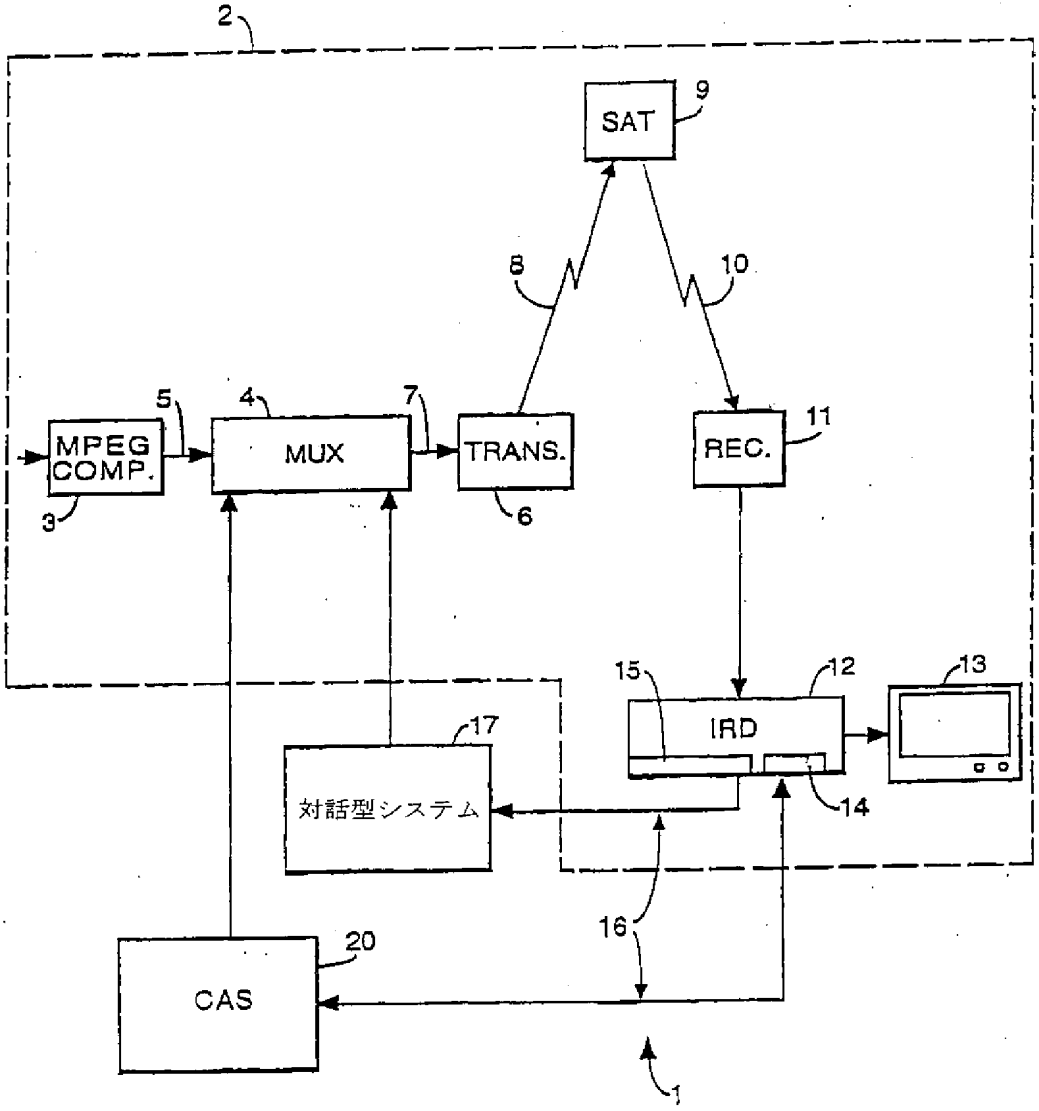
【図７】

デコーダおよびディジタル記録装置のレイアウトを示している。

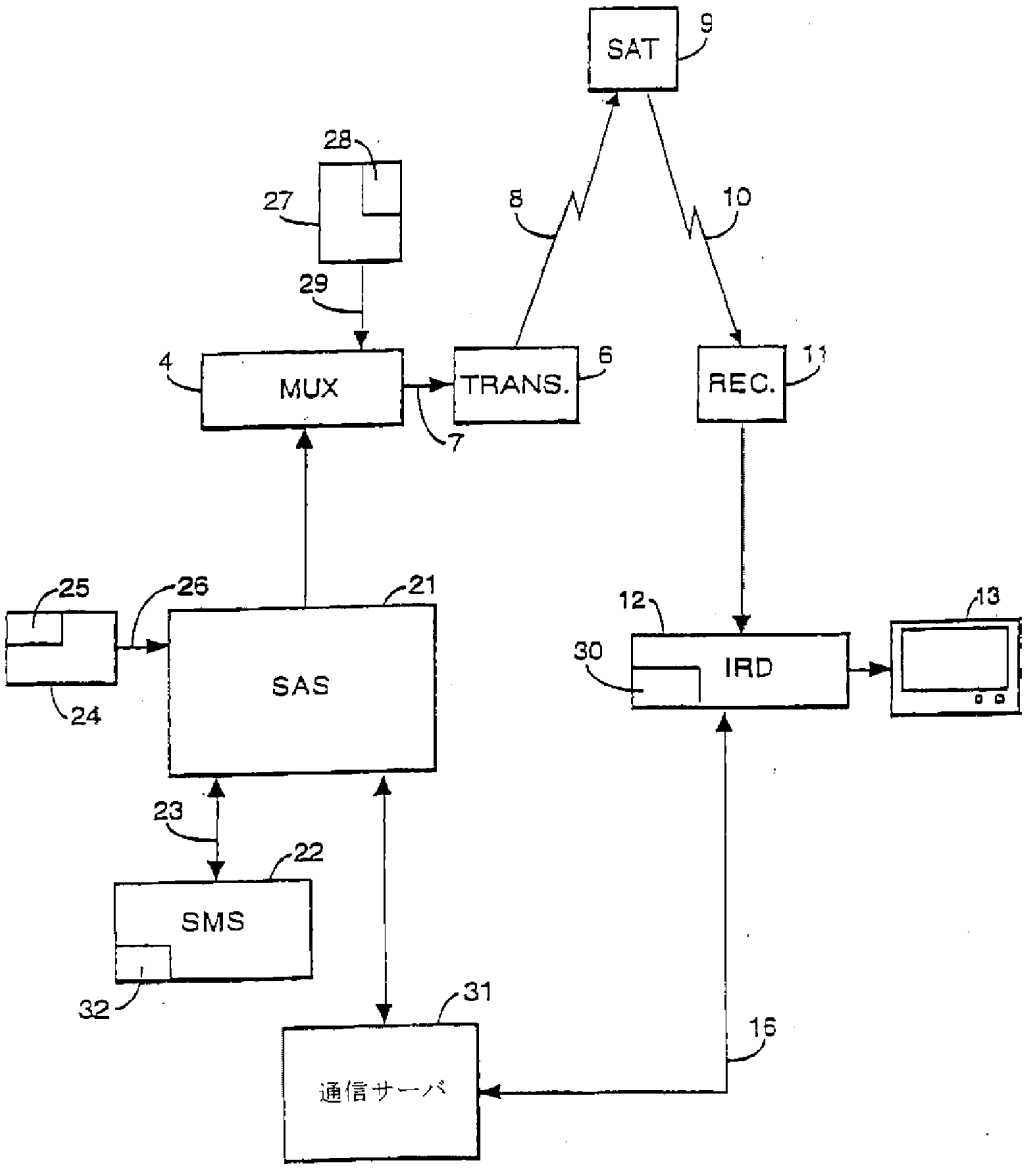
【図８】

デコーダおよびレコーダセキュリティモジュールの個人の専用とすることに関連したステップおよび装置間に安全な通信リンクを生じさせるように実行されるその後の動作に関連したステップを示している。

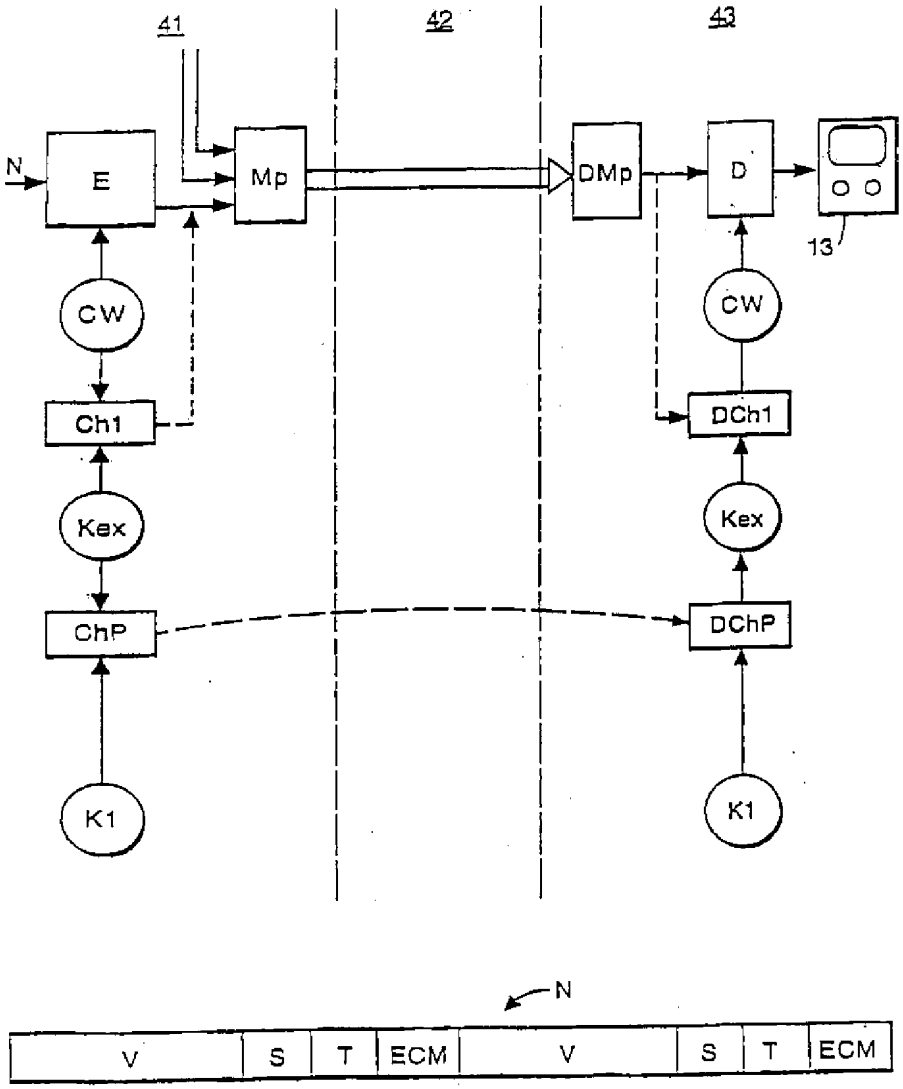
【図１】


2
SAT
9
8
10
MPEG COMP.
5
3
4
MUX
7
TRANS.
6
REC.
11
15
IRD
12
13
14
17
対話型システム
16
CAS
20
1

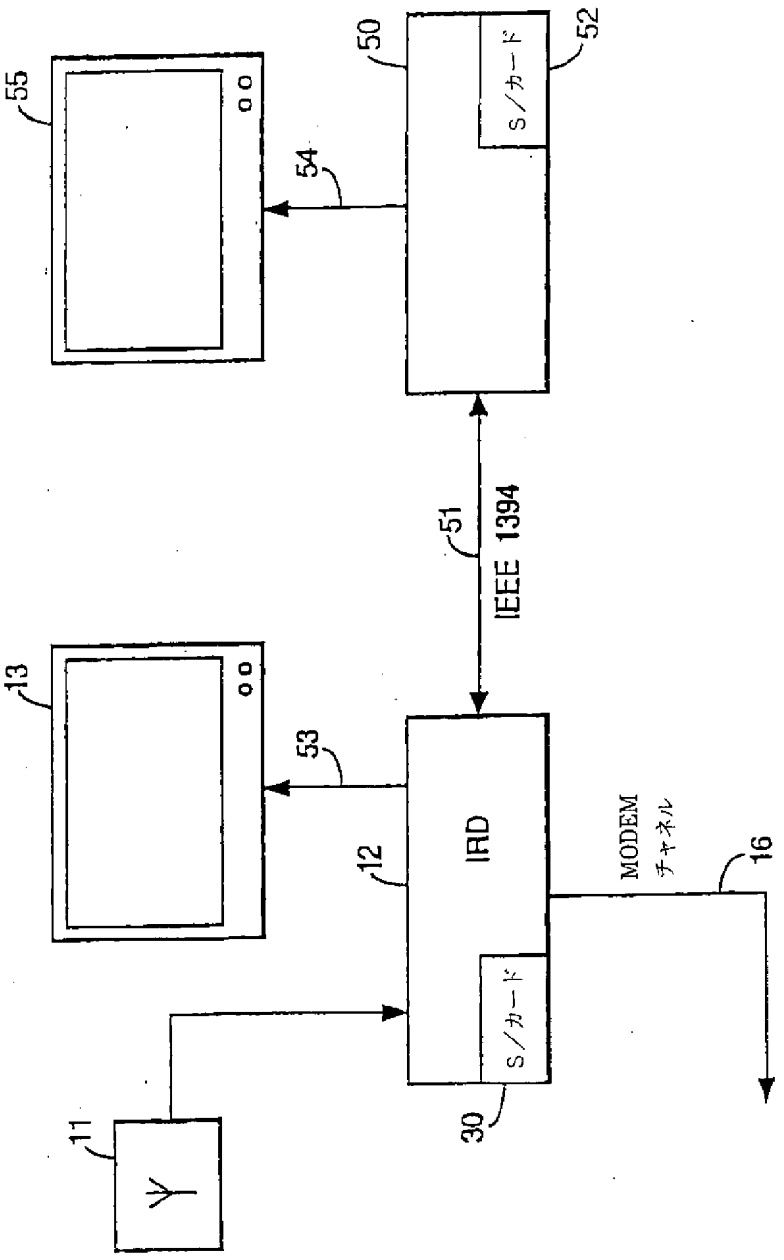
【図２】


SAT
9
28
27
8
10
29
4
MUX
TRANS.
6
REC.
11
7
25
26
21
12
13
30
IRD
SAS
24
23
22
SMS
32
31
16
通信サーバ

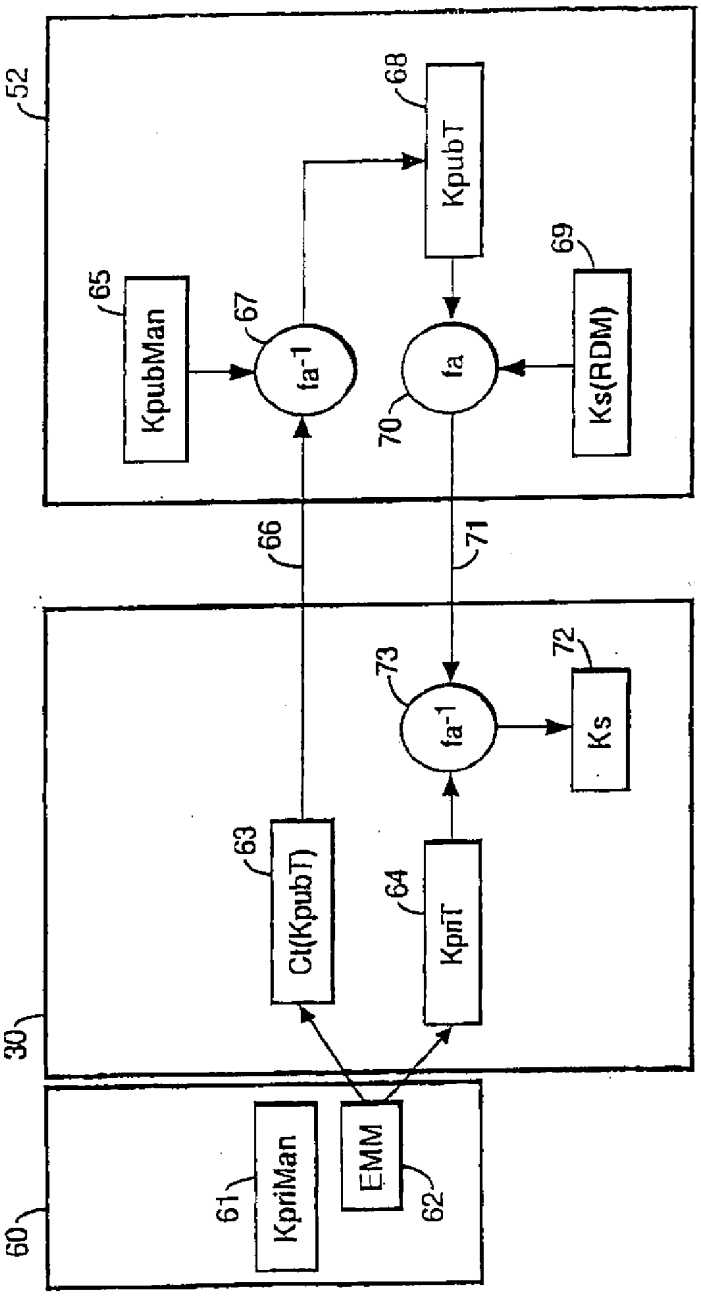
【図３】


41
42
43
N
E
Mp
DMp
D
13
CW
Ch1
Kex
ChP
K1
CW
DCh1
Kex
DChP
K1
N
V
S
T
ECM
V
S
T
ECM

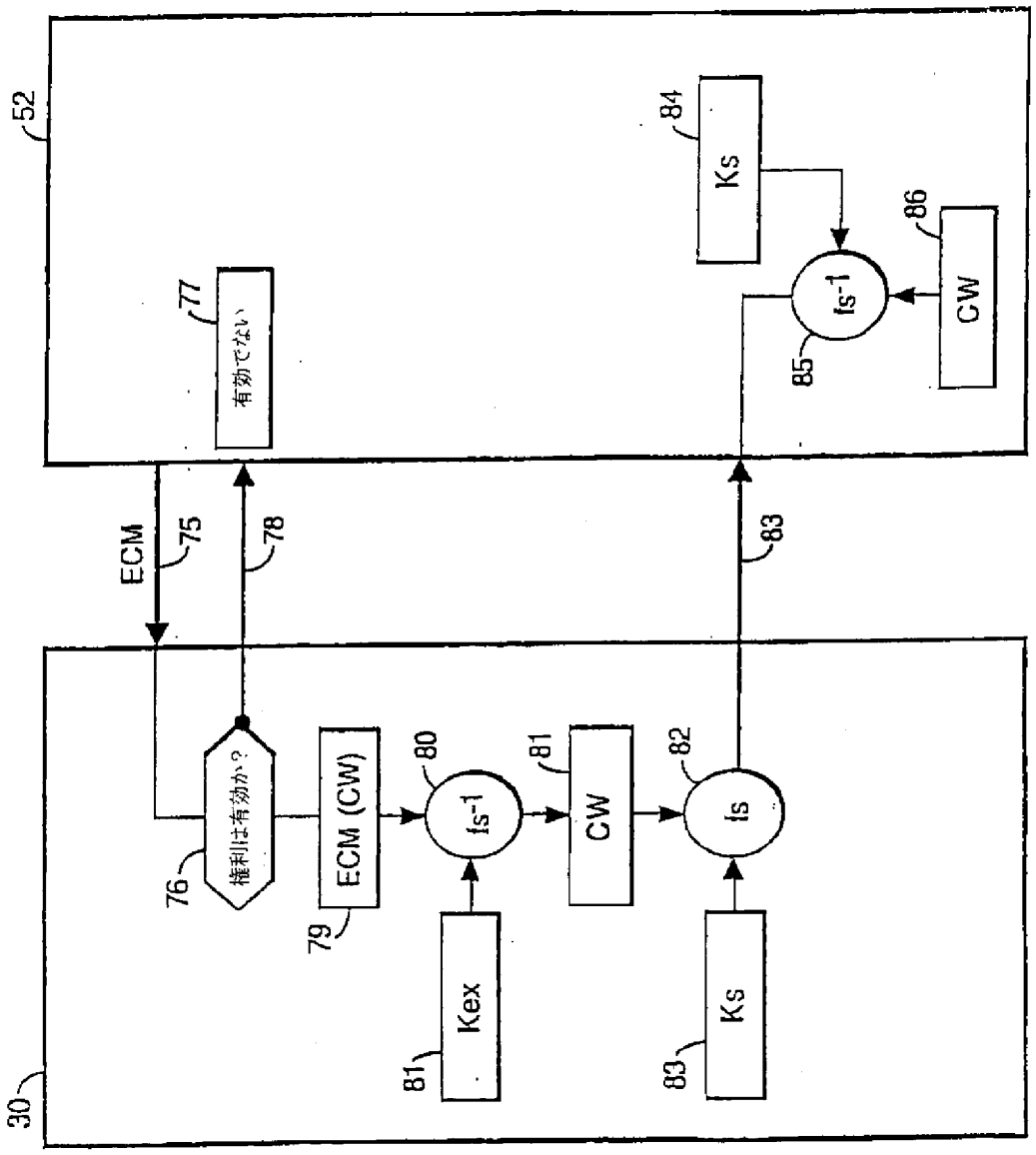
【図４】


55
50
52
S／カード
54
51
IEEE 1394
13
53
12
IRD
MODEM
チャネル
16
S／カード
30
11

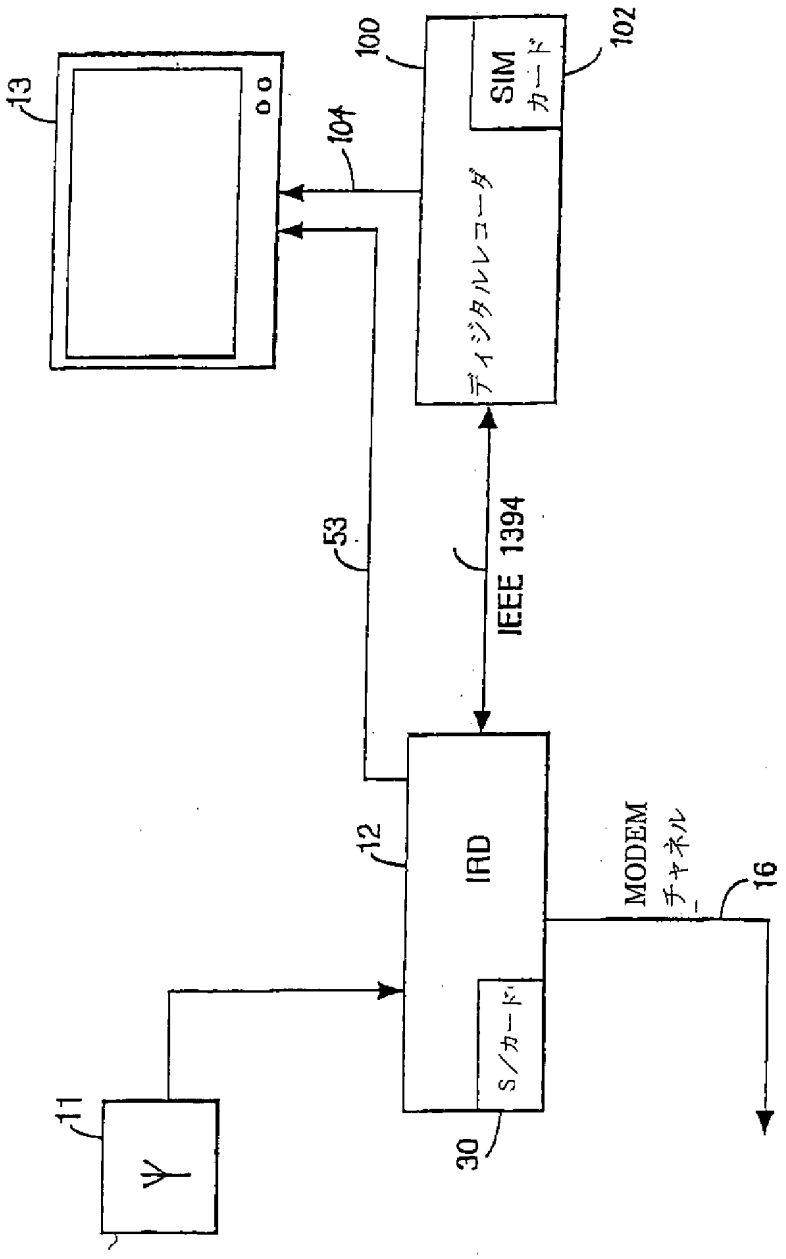
【図５】


52
68
KpubT
65
KpubMan
67
fa-1
fa
69
Ks(RDM)
70
66
71
73
72
fa-1
Ks
63
Ct(KpubT)
64
KpnT
30
61
KpriMan
EMM
62
60

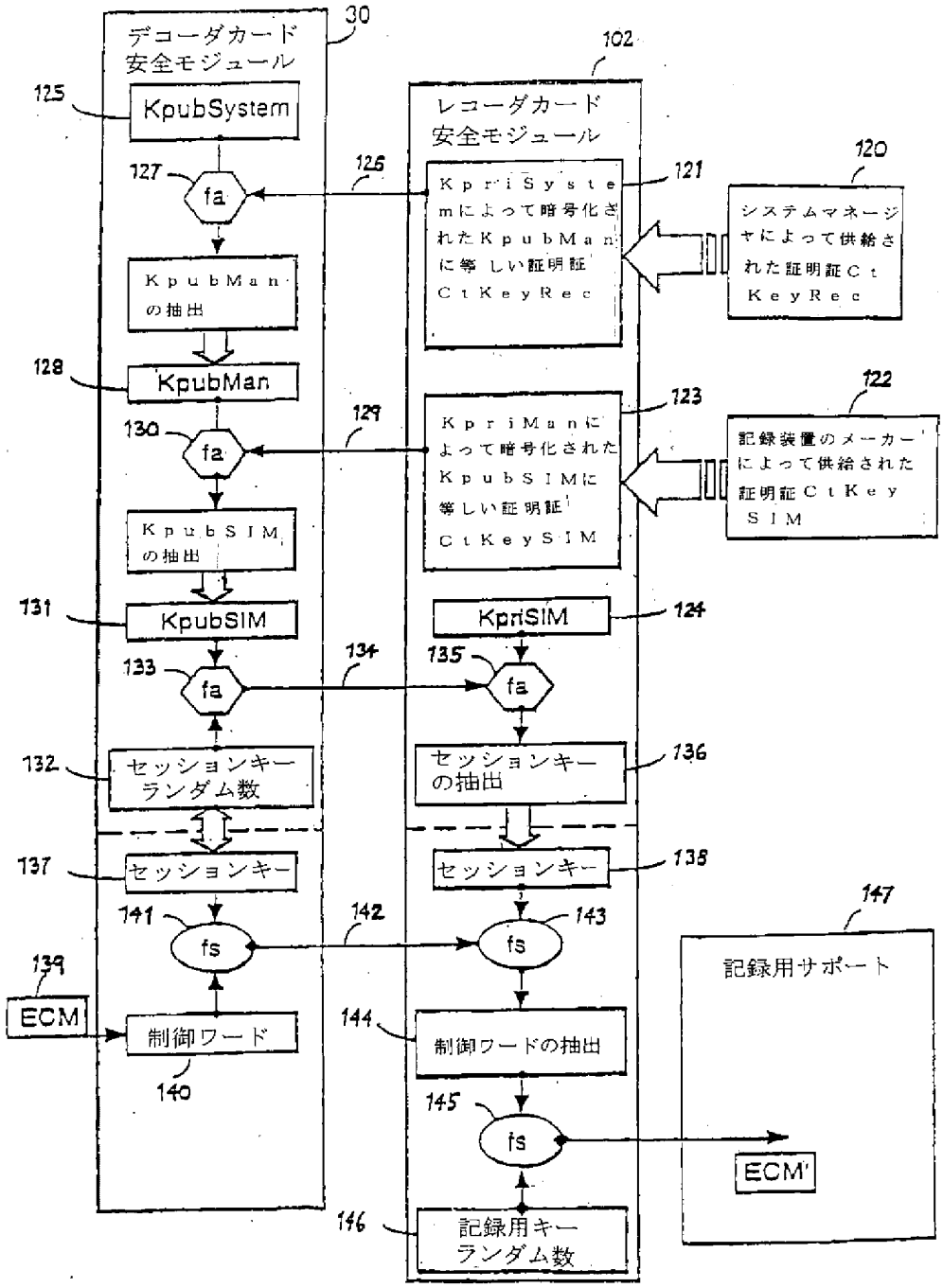
【図６】


52
84
Ks
86
CW
77
有効でない
85
fs-1
ECM
75
78
83
権利は有効か？
76
ECM (CW)
79
80
fs-1
81
CW
82
fs
81
Kex
83
Ks
30

【図７】


13
100
SIM
カード
102
104
ディジタルレコーダ
53
IEEE 1394
12
IRD
MODEM
チャネル
16
S／カード
11
30

【図８】


デコーダカード
安全モジュール
30
KpubSystem
125
127
fa
126
KpubManの抽出
128
KpubMan
130
fa
129
KpubSIMの抽出
131
KpubSIM
133
fa
134
132
セッションキー
ランダム数
137
セッションキー
141
fs
142
139
ECM
制御ワード
140
102
レコーダカード
安全モジュール
KpriSystemによって暗号化されたKpubManに等しい証明証
CtKeyRec
121
120
システムマネージャによって供給された証明証CtKeyRec
KpriManによって暗号化されたKpubSIMに等しい証明証
CtKeySIM
123
122
記録装置のメーカーによって供給された証明証CtKeySIM
KpriSIM
124
135
fa
セッションキーの抽出
136
セッションキー
138
143
fs
制御ワードの抽出
144
145
fs
記録用キーランダム数
146
147
記録用サポート
ECM'

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 99/01323

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 97 38530 A (DIGCO B V ;RIX SIMON PAUL ASHLEY (ZA); GLASSPOOL ANDREW (GB); DAVI) 16 October 1997 (1997-10-16) page 1, line 19 - line 26 page 4, line 1 -page 5, line 10	1,3,5,6, 12,13, 26,27 10,11, 24,25
Y A	US 5 748 732 A (LE BERRE JACQUES ET AL) 5 May 1998 (1998-05-05) column 1, line 17 -column 2, line 16 column 3, line 23 - line 35 column 3, line 64 -column 4, line 43	10,11 9

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 October 1999	05/11/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sindic, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/IB 99/01323

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 97 35430 A (NEWS DATACOM LTD ;TSURIA YOSSEF (IL)) 25 September 1997 (1997-09-25)	10,11
A	page 3, line 1 -page 4, line 16	9
Y	"ENCRYPTION OF INFORMATION TO BE RECORDED SO AS TO PREVENT UNAUTHORIZED PLAYBACK" RESEARCH DISCLOSURE, no. 335, 1 March 1992 (1992-03-01), page 219 XP000301128 ISSN: 0374-4353 the whole document	24,25
A	FORD W ET AL: "PUBLIC-KEY CRYPTOGRAPHY AND OPEN SYSTEMS INTERCONNECTION" IEEE COMMUNICATIONS MAGAZINE, vol. 30, no. 7, 1 July 1992 (1992-07-01), pages 30-35, XP000307910 page 2, paragraph 5	1,13,27
A	FR 2 732 537 A (CANAL PLUS SA) 4 October 1996 (1996-10-04) page 2, line 12 -page 3, line 23	13,18
A	US 4 633 309 A (LI TONY C ET AL) 30 December 1986 (1986-12-30) column 2, line 36 - line 68	9

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ional Application No
PCT/IB 99/01323

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9738530 A	16-10-1997	AU 2506397 A	29-10-1997
		CA 2250833 A	16-10-1997
		CN 1215528 A	28-04-1999
		EP 0891670 A	20-01-1999
		HR 970160 A	28-02-1998
US 5748732 A	05-05-1998	FR 2730372 A	09-08-1996
		EP 0726676 A	14-08-1996
		JP 8251569 A	27-09-1996
WO 9735430 A	25-09-1997	IL 117547 A	14-07-1999
		AU 1317597 A	10-10-1997
		EP 0826288 A	04-03-1998
		GB 2311451 A,B	24-09-1997
FR 2732537 A	04-10-1996	NONE	
US 4633309 A	30-12-1986	CA 1250656 A	28-02-1989

フロントページの続き

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
		Ｈ０４Ｌ　9/00	６０１Ｆ

(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＧＷ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＧＨ，ＧＭ，ＫＥ，ＬＳ，ＭＷ，ＳＤ，ＳＬ，ＳＺ，ＵＧ，ＺＷ)，ＥＡ(ＡＭ，ＡＺ，ＢＹ，ＫＧ，ＫＺ，ＭＤ，ＲＵ，ＴＪ，ＴＭ)，ＡＥ，ＡＬ，ＡＭ，ＡＴ，ＡＵ，ＡＺ，ＢＡ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＣＡ，ＣＨ，ＣＮ，ＣＵ，ＣＺ，ＤＥ，ＤＫ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＤ，ＧＥ，ＧＨ，ＧＭ，ＨＲ，ＨＵ，ＩＤ，ＩＬ，ＩＮ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＣ，ＬＫ，ＬＲ，ＬＳ，ＬＴ，ＬＵ，ＬＶ，ＭＤ，ＭＧ，ＭＫ，ＭＮ，ＭＷ，ＭＸ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＳＬ，ＴＪ，ＴＭ，ＴＲ，ＴＴ，ＵＡ，ＵＧ，ＵＳ，ＵＺ，ＶＮ，ＹＵ，ＺＡ，ＺＷ

Ｆターム(参考)　5C064 DA01 DA12
5J104 AA16 EA06 EA19 NA02 NA03
NA35 NA37

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 7/167, H04L 29/06

A1

(11) International Publication Number: **WO 00/04718**

(43) International Publication Date: 27 January 2000 (27.01.00)

(21) International Application Number: PCT/IB99/01323

(22) International Filing Date: 14 July 1999 (14.07.99)

(30) Priority Data:

98401778.0	15 July 1998 (15.07.98)	EP
98401870.5	22 July 1998 (22.07.98)	EP

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(71) Applicant *(for all designated States except US)*: CANAL+ SOCIETE ANONYME [FR/FR]; 85/89, quai André Citroën, F–75711 Paris Cedex 15 (FR).

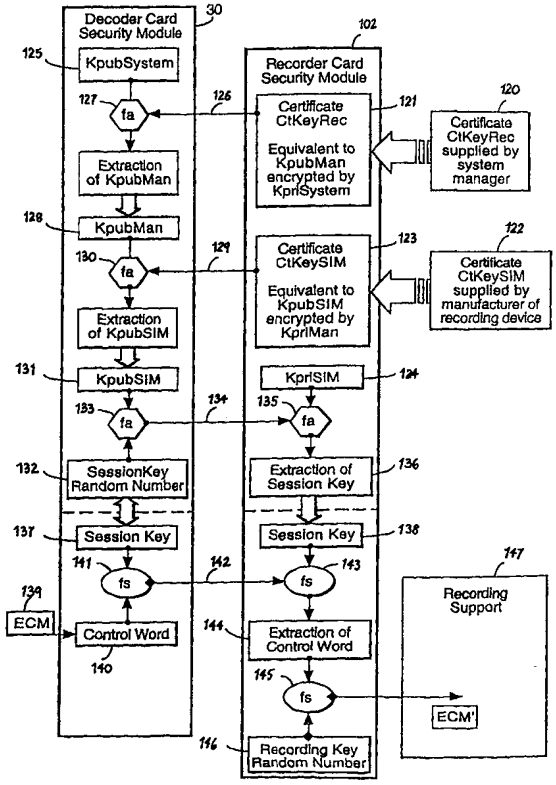
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: DAUVOIS, Jean–Luc [FR/FR]; 19, rue Eugène Manuel, F–75116 Paris (FR). BENARDEAU, Christian [FR/FR]; 13, allée des Puisatiers, F–77600 Bussy Saint Georges (FR).

(74) Agents: COZENS, Paul, Dennis et al.; Mathys & Squire, 100 Gray's Inn Road, London WC1X 8AL (GB).

(54) Title: METHOD AND APPARATUS FOR SECURE COMMUNICATION OF INFORMATION BETWEEN A PLURALITY OF DIGITAL AUDIOVISUAL DEVICES

(57) Abstract

The present invention relates to a method of providing secure communication of information between at least a first and second digital audiovisual device (30, 52) and characterised in that the first device (30) communicates to the second device (52) a certificate Ct(KpubT) comprising a transport public key KpubT encrypted by a management private key KpriMan, the second device (52) decrypting the certificate using an equivalent management public key KpubMan and thereafter using the transport public key KpubT to encrypt information sent to the first device, the first device using an equivalent private key KpriT to decrypt the information. The present invention is particularly applicable to a method of providing secure communication between a first and second decoder.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND APPARATUS FOR SECURE COMMUNICATION OF INFORMATION BETWEEN A PLURALITY OF DIGITAL AUDIOVISUAL DEVICES

The present invention relates to a method and apparatus for secure communication of information between a plurality of digital audiovisual devices connected in a network.

The present invention is particularly applicable to the field of digital television, where scrambled audiovisual information is broadcast to a number of subscribers, each subscriber possessing a decoder or integrated receiver/decoder (IRD) capable of descrambling the transmitted program for subsequent viewing.

In a typical system, scrambled digital audiovisual data is transmitted together with a control word for descrambling of the digital data, the control word itself being encrypted by an exploitation key and transmitted in encrypted form. A decoder receives the scrambled digital data and encrypted control word which uses an equivalent of the exploitation key to decrypt the encrypted control word and thereafter descramble the transmitted data. A paid-up subscriber will receive periodically the exploitation key necessary to decrypt the encrypted control word so as to permit viewing of a particular program. Encryption and decryption keys are conventionally stored in a portable security module, such as a smart card used to personalise the decoder.

A particular problem arises in the case of a user who has two or more decoders since existing subscription management systems often have difficulty in opening a second subscription for the same person at the same address. Consequently, in such circumstances, it would be advantageous to allow two or more decoders to function using the same subscription.

The PCT patent application WO 97/35430 in the name of News Datacom Limited shows one possible solution to this problem. In this system, a pair of decoders are organised in a master/slave configuration. Subscription rights are managed by the

master decoder and its associated smart card. In order to transfer rights to the slave decoder, the slave smart card must be inserted at regular intervals in the master decoder. The disadvantage of this system is that a user is obliged to manually withdraw, recharge and replace the card in the slave decoder.

Other proposed solutions have included the generation of a duplicate smart card containing exactly the same rights as present in a master smart card. Such a solution is also undesirable, since it may not be wished to give exactly the same rights to multiple decoders and since the creation of a clone or duplicate card always incurs the risk fraud.

Another particular problem associated with data transmitted in a digital system lies in its ease of reproduction with no loss of quality. Where a descrambled program is passed via an analogue link (e.g. the " Peritel " link) for viewing and recording by a standard VCR the quality remains no greater than that associated with a standard analogue cassette recording.

By way of contrast, any descrambled digital data passed by a direct digital link to one of the new generation of digital recording devices (for example, a DVHS or DVD recorder) will be of the same quality as the originally transmitted program and may thus be reproduced any number of times without any degradation of image or sound quality. There is therefore a considerable risk that recorded descrambled data will be used as a master recording to make pirate copies.

French Patent Application 95 03859 shows one way of overcoming this problem. In this system, descrambled digital data is never recorded directly on the digital recording medium. Instead, the decoder described in this application forwards the data for recordal on the support medium in its scrambled form. The control word necessary to descramble the data is re-encrypted by means of another key and stored on the recording support with the scrambled data. This new key is known only to the receiver/decoder and replaces the exploitation key needed to obtain the control word for viewing of the program.

The advantage of such a system is that the data is never stored in a "clear" form and cannot be viewed without possession of the new key, stored in the decoder. The system also possesses the advantage that, since the exploitation key changes on a monthly basis, the use of a key chosen by the decoder to re-encrypt the control word registered on the digital tape means that the decoder will still be able to decrypt the control word recorded on the tape even after the end of a subscription month.

The disadvantage of the system proposed in this previous patent application is that the recording can only be viewed in conjunction with that particular decoder. If that decoder breaks down, or is replaced, the recording can no longer be replayed. Equally, it is not possible to play the recording directly in a digital recorder without connecting the decoder in the system.

In order to enable the decoder and recorder to function more effectively it is desired to provide a securised or encrypted communication link between the devices. As will be appreciated from the above description, the interaction of the decoder and recorder may lead to problems, for example, where scrambled transmissions are recorded but where only the decoder possesses the information needed to decrypt such transmissions. The implementation of a secure link between the devices can be used to enable information needed to prepare or play a recording to be passed freely between the devices.

It is an object of the present invention in its general and specific embodiments to overcome some or all of the problems of these prior art systems.

According to the present invention there is providing a method of providing secure communication of information between at least a first and second digital audiovisual device and characterised in that the second device receives a certificate comprising a transport public key encrypted by a management private key, the second device decrypting the certificate using an equivalent management public key and thereafter using the transport public key to encrypt information sent to the first device, the first device using an equivalent private key to decrypt the information.

In such a method, the first device can assume the role of a master device, personalised with a certificate generated using a management private key. The management private key is held in secret by the system manager and may not be derived from the information stored in the certificate. The second device can assume the role of a slave device. Information encrypted by the transport public key held by the second device may only be decrypted by the equivalent private key held by the first device. As will be described below, this information may thereafter be used to set up a secure bi-directional link to transfer subscription rights and other information.

Advantageously, the transport private/public key pair are uniquely associated with the first and second device pair. This ensures complete security of encrypted messages transmitted to the first device.

As will be appreciated, whilst the use of unique keys enables an increased level of security it may be decided in some cases to use non-unique keys, for example, for different pairs of devices distributed in different territories, where the security risk associated with such duplication is relatively low.

Preferably, the encrypted information sent by the second device comprises a session key, in particular, a session key generated by the second device and usable in conjunction with a symmetric encryption algorithm. This key, which may be generated at the initiation of a communication session for transfer of subscription can thereafter be used for bi-directional communication of information between the first and second devices.

In an alternative embodiment a session key pair corresponding to a private/public key pair of an asymmetric algorithm may be used.

The advantage of a changeable symmetric session key lies in the increased level of security that such a key provides as well as the possibility of bi-directional communication that it enables. Other embodiments are nevertheless possible, for

example, in which transmission related information is directly encrypted using the transport public key held by the second device.

In one embodiment, the session key is used by the first device to encrypt control word information subsequently communicated to the second device. In such an embodiment, the second device decrypts the control word information using the equivalent session key and thereafter descrambles an associated transmission or programme for display.

In one embodiment, prior to the communication of the first certificate, the second device receives a secondary system certificate comprising the management public key encrypted by a system private key, the second device decrypting the system certificate using a system public key so as to obtain the management public key used thereafter to decrypt the encrypted transport public key.

This embodiment may be implemented, for example, where a different source for the first and second devices exists. The system private key may be held in secret by, for example, the source of the second device. A system certificate will only be issued in the event that the second device source is sure of the integrity of security at the first device source. Thereafter, a designated first device source will embed this certificate in all first device smart cards, such that a second device smart card can authenticate the origin of such cards.

As will be understood, the second device source need only know the management public key of the first device source in order to generate a system certificate and neither party needs to share its private encryption keys in carrying out these certifying operations.

The secure communication link between the devices may be used to convey many different types of information, including different information relating to descrambling a transmission or even other matters. In particular, whilst the above embodiments discuss the use of a session key in the encryption and communication of control word

information, other embodiments are possible. For example, audio and/or visual data to be recorded may be directly encrypted by the first device using a session key and communicated directly to the second device for decryption and display.

Other embodiments may use the secure communication link to transfer, for example, exploitation keys present in the first device such that the second device can carry out all operations to decrypt control word information and descramble a transmission in the same manner as the first device.

Whilst the above description has described encryption and decryption operations in relation to a first and second device it is to be understood that these operations and, in particular the keys needed in such operations, need not necessarily be managed or held by elements permanently integrated in the devices themselves.

In particular, in a preferred embodiment, the first and second devices further comprise first and second portable security modules used to carry out some or all of the encryption or decryption steps described above.

Such portable security devices can take any convenient form depending on the physical size and characteristics of the device. For example, whilst in some cases a smart card equivalent to a bank card may be used, other formats such as PCMCIA type cards are equally possible.

The physical communication link between the two devices may take many forms, for example, a radio, telephone or infra-red link. However, preferably, the communication link is implemented by connection of the first and second decoders on a bus, for example, a IEEE 1394 bus link.

Whilst the invention has been described with reference to a first and second device, it will be appreciated that the same principal may be used to set up a chain of communication between a series of such devices, e.g. between a single master device and a plurality of slave devices.

The present invention is particularly, but not exclusively, applicable to the implementation of secure communication link between a first and second decoder. However, other applications of the invention for use with other digital audiovisual devices may be envisaged, for example, to encrypt information from a decoder to a digital VCR, between two digital VCRs etc.

In one preferred embodiment, the devices comprise a decoder device and a recorder device. Thus, the present invention extends to a method of providing secure communication of information between a decoder device and a recorder device and characterised in that a first one of the devices communicates to the second device a certificate comprising a device public key encrypted by a management private key, the second device decrypting the certificate using an equivalent management public key and thereafter using the device public key to encrypt information sent to the first device, the first device using an equivalent device private key to decrypt the information.

In such a method, the first device initiating the communication is personalised with a certificate generated by a management private key. The management private key is held in secret by the source responsible for this device (e.g. a recorder device manufacturer) and may not be derived from the information stored in the certificate. The communication of such a certificate therefore provides the second device with a level of assurance concerning the identity and origin of the device initiating the communication.

In addition, the information encrypted by the device public key held by the second device may only be decrypted by the equivalent private key held by the first device thereby enabling the second device to communicate in confidence information to the first device. As will be described below, this information may thereafter be used to set up a secure bi-directional link.

Preferably, prior to the communication of the first device certificate, the first device communicates to the second device a system certificate comprising the management

public key encrypted by a system private key, the second device decrypting the system certificate using a system public key so as to obtain the management public key used thereafter to decrypt the device certificate.

The private system key may be held in secret by, for example, the source of the second device (e.g. a broadcast system manager responsible for the decoder). A system certificate will only be issued in the event that the second device source is sure of the integrity of security at the first device source, that is, that the second device source is sure that the management private key is only known to by the first device source and that the necessary measures have been put in place to keep this key secret.

As will be understood, the second device source need only know the public management key of the first device source in order to generate a system certificate and neither party needs to share its private encryption keys in carrying out these certifying operations.

Advantageously, the device private/public key pair are uniquely associated with the first device. This ensures complete security of encrypted messages transmitted to the first device. Further advantageously, the management private/public key pair are uniquely associated with the source of the first device and the system private/public key pair (if present) are uniquely associated with the source of the second device.

As will be appreciated, although the use of unique keys enables an increased level of security, it may be decided in some cases to use non-unique keys. For example, in the case of high volume of production of first devices, certain of these devices may share the same device private key if such devices are distributed in different territories, since the security risk associated with such duplication is relatively low.

Preferably, the encrypted information sent by the second device comprises a session key, in particular, a session key generated by the second device and usable in conjunction with a symmetric encryption algorithm. This key, which may be

generated at the initiation of a recording session can thereafter be used for bi-directional communication of information between the first and second devices.

In an alternative embodiment, a session key pair corresponding to a private/public key pair of an asymmetric algorithm may be used.

The advantage of a changeable session key lies in the increased level of security that such a key provides as well as the possibility of secure bi-directional communication that it enables if a symmetric session key is chosen. Other embodiments are nevertheless possible, for example, in which information associated with a recording operation may be directly encrypted using the device public key held by the second device.

In one embodiment, the session key is used by the decoder device to encrypt control word information subsequently communicated to the recorder device. In such an embodiment, the recorder device may decrypt the control word information using the equivalent session key and thereafter re-encrypt the control word information using a recording encryption key, the re-encrypted control word information being stored by the recorder on a recording support medium together with the scrambled transmission data associated with that control word information.

The encryption of control word information using a recording key held by the recorder device enables the recorder device to replay at any time a recorded scrambled transmission independently of the decoder device originally used to receive and forward the transmission.

Advantageously, the recorder device communicates to the decoder device a copy of the recording encryption key. This may be conveniently encrypted by the session key prior to communication. This copy may thereafter be decrypted by the decoder and a back-up copy of the recording key stored in the decoder.

As will be understood, the secure communication link may be used to convey many

different types of information. In particular, whilst the above embodiments discuss the use of a session key in the encryption and communication of control word information for use in a recording operation, other embodiments are possible. For example, audio and/or visual data to be recorded may be directly encrypted by the decoder using a session key and communicated to the recorder for decryption and subsequent re-encryption prior to recordal.

Other embodiments may use the secure communication link to transfer, for example, decoder exploitation keys to the recorder device such that the recorder device can carry out all operations to decrypt control word information and/or descramble a transmission prior to its recordal in a re-encrypted or rescrambled form on a recording support medium.

Whilst the above description has described encryption and decryption operations in relation to a decoder device or recorder device it is to be understood that these operations and, in particular the keys needed in such operations, need not necessarily handled by elements permanently integrated in the devices themselves.

In particular, in a preferred embodiment, the recorder and/or decoder device may further comprise a portable security module associated with that device and used to carry out some or all of the encryption or decryption steps described above.

Such portable security devices can take any convenient form depending on the physical size and characteristics of the decoder or recorder. For example, a smart card or PCMCIA type card may be used with a decoder and a SIM card or similar with a recorder.

In a particularly preferred embodiment of the invention, the first device corresponds to a recorder device and the second device to a decoder device. In such a system the decoder system manager will have ultimate control, for example, over generation of system certificates issued to recorder manufacturers. Similarly communication will be initiated by the recorder, the decoder only communicating an encrypted message

containing the information that will be needed to set up a bi-directional communication in the event that the recorder has communicated correct system and/or management certificates.

Whilst the invention is particularly convenient where the decoder and recorder are physically separate, the invention may equally be used in a combination recorder/decoder apparatus to provide, for example, a secure bus link between the recorder and decoder devices within the combined apparatus.

The present invention is particularly but not exclusively adapted for use with a digital television transmission system in which the decoders are adapted to receive a digital television transmission.

The present invention has been described above in relation to a method of communication. The invention equally extends to a first and second device adapted for use in such a method and one or more portable security modules adapted for use in such a system.

Suitable algorithms for use in this invention for generating private/public keys may include, for example, RSA or Diffie-Hellman, and suitable symmetric key algorithms may include DES type algorithms, for example. However, unless obligatory in view of the context or unless otherwise specified, no general distinction is made between keys associated with symmetric algorithms and those associated with public/private algorithms.

The terms "scrambled" and "encrypted" and "control word" and "key" have been used at various parts in the text for the purpose of clarity of language. However, it will be understood that no fundamental distinction is to be made between "scrambled data" and "encrypted data" or between a "control word" and a "key". Similarly, the term "equivalent key" is used to refer to a key adapted to decrypt data encrypted by a first mentioned key, or vice versa.

The term "receiver/decoder" or "decoder" as used herein may connote a receiver for receiving either encoded or non-encoded signals, for example, television and/or radio signals, which may be broadcast or transmitted by some other means. The term may also connote a decoder for decoding received signals. Embodiments of such decoders may also include a decoder integral with the receiver for decoding the received signals, for example, in a "set-top box", a decoder functioning in combination with a physically separate receiver, or such a decoder including additional functions, such as a web browser or a video recorder or a television.

As used herein, the term "digital transmission system" includes any transmission system for transmitting or broadcasting for example primarily audiovisual or multimedia digital data. Whilst the present invention is particularly applicable to a broadcast digital television system, the invention may also be applicable to a fixed telecommunications network for multimedia internet applications, to a closed circuit television, and so on.

As used herein, the term "digital television system" includes for example any satellite, terrestrial, cable and other system.

There will now be described, by way of example only, a number of embodiments of the invention, with reference to the following figures, in which:

Figure 1 shows the overall architecture of a digital TV system according to this embodiment;

Figure 2 shows the architecture of the conditional access system of Figure 1;

Figure 3 shows the encryption levels in the conditional access system;

Figure 4 shows the layout of a first and second decoder;

Figure 5 shows the steps associated with setting up a secure communication link

between the first and second decoder; and

Figure 6 shows the operation of the first and second decoder in transferring control word information via the secure communication link.

Figure 7 shows the layout of a decoder and digital recording device; and

Figure 8 shows the steps associated with the personalisation of decoder and recorder security modules and with the subsequent operations carried out to set up a secure communication link between the devices.

An overview of a digital television broadcast and reception system 1 is shown in Figure 1. The invention includes a mostly conventional digital television system 2 which uses the MPEG-2 compression system to transmit compressed digital signals. In more detail, MPEG-2 compressor 3 in a broadcast centre receives a digital signal stream (for example a stream of audio or video signals). The compressor 3 is connected to a multiplexer and scrambler 4 by linkage 5. The multiplexer 4 receives a plurality of further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter 6 of the broadcast centre via linkage 7, which can of course take a wide variety of forms including telecom links.

The transmitter 6 transmits electromagnetic signals via uplink 8 towards a satellite transponder 9, where they are electronically processed and broadcast via a notional downlink 10 to earth receiver 11, conventionally in the form of a dish owned or rented by the end user. The signals received by receiver 11 are transmitted to an integrated receiver/decoder 12 owned or rented by the end user and connected to the end user's television set 13. The receiver/decoder 12 decodes the compressed MPEG-2 signal into a television signal for the television set 13.

A conditional access system 20 is connected to the multiplexer 4 and the receiver/decoder 12, and is located partly in the broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or

more broadcast suppliers. A smartcard, capable of decrypting messages relating to commercial offers (that is, one or several television programmes sold by the broadcast supplier), can be inserted into the receiver/decoder 12. Using the decoder 12 and smartcard, the end user may purchase events in either a subscription mode or a pay-per-view mode.

An interactive system 17, also connected to the multiplexer 4 and the receiver/decoder 12 and again located partly in the broadcast centre and partly in the decoder, may be provided to enable the end user to interact with various applications via a modemmed back channel 16.

The conditional access system 20 will now be described in more detail. With reference to Figure 2, in overview the conditional access system 20 includes a Subscriber Authorization System (SAS) 21. The SAS 21 is connected to one or more Subscriber Management Systems (SMS) 22, one SMS for each broadcast supplier, for example by a respective TCP-IP linkage 23 (although other types of linkage could alternatively be used). Alternatively, one SMS could be shared between two broadcast suppliers, or one supplier could use two SMSs, and so on.

First encrypting units in the form of ciphering units 24 utilising "mother" smartcards 25 are connected to the SAS by linkage 26. Second encrypting units again in the form of ciphering units 27 utilising mother smartcards 28 are connected to the multiplexer 4 by linkage 29. The receiver/decoder 12 receives a portable security module, for example in the form of "daughter" smartcard 30. It is connected directly to the SAS 21 by Communications Servers 31 via the modemmed back channel 16. The SAS sends, amongst other things, subscription rights to the daughter smartcard on request.

The smartcards contain the secrets of one or more commercial operators. The "mother" smartcard encrypts different kinds of messages and the "daughter" smartcards decrypt the messages, if they have the rights to do so.

The first and second ciphering units 24 and 27 comprise a rack, an electronic VME card with software stored on an EEPROM, up to 20 electronic cards and one smartcard 25 and 28 respectively, for each electronic card, one card 28 for encrypting the ECMs and one card 25 for encrypting the EMMs.

The operation of the conditional access system 20 of the digital television system will now be described in more detail with reference to the various components of the television system 2 and the conditional access system 20.

Multiplexer and Scrambler

With reference to Figures 1 and 2, in the broadcast centre, the digital audio or video signal is first compressed (or bit rate reduced), using the MPEG-2 compressor 3. This compressed signal is then transmitted to the multiplexer and scrambler 4 via the linkage 5 in order to be multiplexed with other data, such as other compressed data.

The scrambler generates a control word used in the scrambling process and included in the MPEG-2 stream in the multiplexer. The control word is generated internally and enables the end user's integrated receiver/decoder 12 to descramble the programme.

Access criteria, indicating how the programme is commercialised, are also added to the MPEG-2 stream. The programme may be commercialised in either one of a number of "subscription" modes and/or one of a number of "Pay Per View" (PPV) modes or events. In the subscription mode, the end user subscribes to one or more commercial offers, or "bouquets", thus getting the rights to watch every channel inside those bouquets. In the preferred embodiment, up to 960 commercial offers may be selected from a bouquet of channels.

In the Pay Per View mode, the end user is provided with the capability to purchase events as he wishes. This can be achieved by either pre-booking the event in advance ("pre-book mode"), or by purchasing the event as soon as it is broadcast ("impulse

mode"). In the preferred embodiment, all users are subscribers, whether or not they watch in subscription or PPV mode, but of course PPV viewers need not necessarily be subscribers.

Entitlement Control Messages

Both the control word and the access criteria are used to build an Entitlement Control Message (ECM). This is a message sent in relation with a scrambled program; the message contains a control word (which allows for the descrambling of the program) and the access criteria of the broadcast program. The access criteria and control word are transmitted to the second encrypting unit 27 via the linkage 29. In this unit, an ECM is generated, encrypted and transmitted on to the multiplexer and scrambler 4. During a broadcast transmission, the control word typically changes every few seconds, and so ECMs are also periodically transmitted to enable the changing control word to be descrambled. For redundancy purposes, each ECM typically includes two control words; the present control word and the next control word.

Each service broadcast by a broadcast supplier in a data stream comprises a number of distinct components; for example a television programme includes a video component, an audio component, a sub-title component and so on. Each of these components of a service is individually scrambled and encrypted for subsequent broadcast to the transponder 9. In respect of each scrambled component of the service, a separate ECM is required. Alternatively, a single ECM may be required for all of the scrambled components of a service. Multiple ECMs are also generated in the case where multiple conditional access systems control access to the same transmitted program.

Entitlement Management Messages (EMMs)

The EMM is a message dedicated to an individual end user (subscriber), or a group of end users. Each group may contain a given number of end users. This organisation as a group aims at optimising the bandwidth; that is, access to one group

can permit the reaching of a great number of end users.

Various specific types of EMM can be used. Individual EMMs are dedicated to individual subscribers, and are typically used in the provision of Pay Per View services; these contain the group identifier and the position of the subscriber in that group.

Group subscription EMMs are dedicated to groups of, say, 256 individual users, and are typically used in the administration of some subscription services. This EMM has a group identifier and a subscribers' group bitmap.

Audience EMMs are dedicated to entire audiences, and might for example be used by a particular operator to provide certain free services. An "audience" is the totality of subscribers having smartcards which bear the same conditional access system identifier (CA ID). Finally, a "unique" EMM is addressed to the unique identifier of the smartcard.

EMMs may be generated by the various operators to control access to rights associated with the programs transmitted by the operators as outlined above. EMMs may also be generated by the conditional access system manager to configure aspects of the conditional access system in general.

Programme Transmission

The multiplexer 4 receives electrical signals comprising encrypted EMMs from the SAS 21, encrypted ECMs from the second encrypting unit 27 and compressed programmes from the compressor 3. The multiplexer 4 scrambles the programmes and sends the scrambled programmes, the encrypted EMMs and the encrypted ECMs to a transmitter 6 of the broadcast centre via the linkage 7. The transmitter 6 transmits electromagnetic signals towards the satellite transponder 9 via uplink 8.

Programme Reception

The satellite transponder 9 receives and processes the electromagnetic signals transmitted by the transmitter 6 and transmits the signals on to the earth receiver 11, conventionally in the form of a dish owned or rented by the end user, via downlink 10. The signals received by receiver 11 are transmitted to the integrated receiver/decoder 12 owned or rented by the end user and connected to the end user's television set 13. The receiver/decoder 12 demultiplexes the signals to obtain scrambled programmes with encrypted EMMs and encrypted ECMs.

If the programme is not scrambled, that is, no ECM has been transmitted with the MPEG-2 stream, the receiver/decoder 12 decompresses the data and transforms the signal into a video signal for transmission to television set 13.

If the programme is scrambled, the receiver/decoder 12 extracts the corresponding ECM from the MPEG-2 stream and passes the ECM to the "daughter" smartcard 30 of the end user. This slots into a housing in the receiver/decoder 12. The daughter smartcard 30 controls whether the end user has the right to decrypt the ECM and to access the programme. If not, a negative status is passed to the receiver/decoder 12 to indicate that the programme cannot be descrambled. If the end user does have the rights, the ECM is decrypted and the control word extracted. The decoder 12 can then descramble the programme using this control word. The MPEG-2 stream is decompressed and translated into a video signal for onward transmission to television set 13.

Subscriber Management System (SMS)

A Subscriber Management System (SMS) 22 includes a database 32 which manages, amongst others, all of the end user files, commercial offers, subscriptions, PPV details, and data regarding end user consumption and authorization. The SMS may be physically remote from the SAS.

Each SMS 22 transmits messages to the SAS 21 via respective linkage 23 which imply modifications to or creations of Entitlement Management Messages (EMMs)

to be transmitted to end users.

The SMS 22 also transmits messages to the SAS 21 which imply no modifications or creations of EMMs but imply only a change in an end user's state (relating to the authorization granted to the end user when ordering products or to the amount that the end user will be charged).

The SAS 21 sends messages (typically requesting information such as call-back information or billing information) to the SMS 22, so that it will be apparent that communication between the two is two-way.

Subscriber Authorization System (SAS)

The messages generated by the SMS 22 are passed via linkage 23 to the Subscriber Authorization System (SAS) 21, which in turn generates messages acknowledging receipt of the messages generated by the SMS 21 and passes these acknowledgements to the SMS 22.

In overview the SAS comprises a Subscription Chain area to give rights for subscription mode and to renew the rights automatically each month, a Pay Per View Chain area to give rights for PPV events, and an EMM Injector for passing EMMs created by the Subscription and PPV chain areas to the multiplexer and scrambler 4, and hence to feed the MPEG stream with EMMs. If other rights are to be granted, such as Pay Per File (PPF) rights in the case of downloading computer software to a user's Personal Computer, other similar areas are also provided.

One function of the SAS 21 is to manage the access rights to television programmes, available as commercial offers in subscription mode or sold as PPV events according to different modes of commercialisation (pre-book mode, impulse mode). The SAS 21, according to those rights and to information received from the SMS 22, generates EMMs for the subscriber.

The EMMs are passed to the Ciphering Unit (CU) 24 for ciphering with respect to the management and exploitation keys. The CU completes the signature on the EMM and passes the EMM back to a Message Generator (MG) in the SAS 21, where a header is added. The EMMs are passed to a Message Emitter (ME) as complete EMMs. The Message Generator determines the broadcast start and stop time and the rate of emission of the EMMs, and passes these as appropriate directions along with the EMMs to the Message Emitter. The MG only generates a given EMM once; it is the ME which performs cyclic transmission of the EMMs.

On generation of an EMM, the MG assigns a unique identifier to the EMM. When the MG passes the EMM to the ME, it also passes the EMM ID. This enables identification of a particular EMM at both the MG and the ME.

In systems such as simulcrypt which are adapted to handle multiple conditional access systems e.g. associated with multiple operators, EMM streams associated with each conditional access system are generated separately and multiplexed together by the multiplexer 4 prior to transmission.

Encryption Levels of the Broadcast System

Referring now to Figure 3, a simplified outline of the encryption levels in a standard broadcast system will now be described. The stages of encryption associated with the broadcast of the digital data are shown at 41, the transmission channel (eg a satellite link as described above) at 42 and the stages of decryption at the receiver at 43.

The digital data N is scrambled by a control word CW before being transmitted to a multiplexer Mp for subsequent transmission. As will be seen from the lower part of Figure 3, the transmitted data includes an ECM comprising, inter alia, the control word CW as encrypted by an encrypter Ch1 controlled by an exploitation key Kex. At the receiver/decoder, the signal passes by a demultiplexer DMp and descrambler D before being passed to a television 13 for viewing. A decryption unit DCh1 also possessing the key Kex decrypts the ECM in the demultiplexed signal to obtain the

control word CW subsequently used to descramble the signal.

For security reasons, the control word CW embedded in the encrypted ECM changes on average every 10 seconds or so. In contrast, the first encryption key Kex used by the receiver to decode the ECM is changed every month or so by means of an operator EMM. The encryption key Kex is encrypted by a second unit ChP using a personalised group key K1(GN). If the subscriber is one of those chosen to receive an updated key Kex, a decryption unit DChP in the decoder security module will decrypt the message using its group key K1(GN) to obtain that month's key Kex.

The decryption units DChp and DCh1 and the associated keys are held on a security module associated with the decoder, in this case the smart card 30 provided to the subscriber and inserted in a smart card reader in the decoder. The keys may be generated, for example, according to any generally used symmetric key algorithm or in accordance with a customised symmetric key algorithm.

As will be described, different keys may be associated with different operators or broadcasters as well as with the conditional access system supplier. In the above description, a group key K1(GN) is held by the smart card associated with the decoder and used to decrypt EMM messages. In practice, different operators will have different subscriber unique keys K1 (Op1, GN), K1 (Op2, GN) etc. Each group key is generated by an operator and diversified by a value associated with the group to which the subscriber belongs.

Different memory zones in the smart card hold the keys for different operators. Each operator may also have a unique key associated solely with the smart card in question and an audience key for all subscribers to the services provided by that operator (see above).

In addition, a set of keys may also be held by the manager of the conditional access system. In particular, a given smart card may include a user specific key K0 (NS) and an audience key K1 (C), common to all smart cards. Whilst the operator keys

are generally used to decode EMM messages associated with broadcast rights, the conditional access manager keys may be used to decrypt EMM messages associated with changes to conditional access system in general, as will be described below.

The above description of the system shown in Figure 3 relates to the implementation of access control in a broadcast system in which transmissions are descrambled by a single decoder and displayed on a single television display. Referring to Figure 4, a first and second decoder configuration will now be described.

Decoder Configuration

As before, a decoder 12 receives scrambled broadcast transmissions via a receiver 11. The decoder includes a portable security module 30, which may conveniently take the form of a smart card, but which may comprise any other suitable memory or microprocessor portable device. The decoder 12 is connected to a modem channel 16, for example, for communicating with servers handling conditional access information and is also adapted to pass descrambled audiovisual display information, e.g. via a Peritel link 53, to a television 13.

The system additionally includes a dependent or slave decoder 50 adapted to communicate with the decoder 12, for example, via an IEEE 1394 bus 51. The decoder 50 may include a connection (not shown) to the receiver 11 or to another satellite receiver to directly receive scrambled broadcast transmissions. Alternatively, this information may be passed from the first decoder 12 via the connection 51.

The second decoder 50 is further adapted to function with a portable security module 52. The portable security module 52 may conveniently be implemented as smart card. However, any portable memory and/or microprocessor device as is conventionally known, such as a PCMCIA card, a microprocessor key etc. may be used. The operation of this module 52 in descrambling transmissions will be explained below.

The decoder 50 also includes a link 54 to a television display 55 used to display descrambled transmissions. Whilst the elements of the decoders 12, 50 and the displays 13, 55 have been indicated separately, it is envisaged that some or all of these elements may be merged, for example, to provide a combined decoder/television set.

Secure Communication between Decoders

As set out in the introduction, in order to avoid problems relating to management of subscription data, it is desirable that only a single subscription is opened for the owner of the two decoders 12, 50. In the case where the decoder 12 is the principal or first decoder in the system, smart card 30 will be personalised to receive the monthly exploitation key Kex as described above in relation to Figure 3. In order to enable the decoder 50 to descramble and display a transmission via the display 55 it will be necessary to communicate certain information from the security module 30 to the security module 52 to enable this descrambling to be carried out.

In the present embodiment, the smart card 30 decrypts the ECM messages associated with a transmission so as to obtain the control word CW value. This control word value is then communicated in an encrypted form via the link 51 to the decoder 50 and smart card 52, where it is used by the decoder 50 and smart card 52 to descramble the transmission and display the programme via the display 55.

Embodiments other than this control word embodiment may nevertheless be envisaged, for example, in which a copy of the monthly exploitation Kex is passed to the decoder and smart card 50, 52 to enable the decoder 50 to operate independently thereafter.

As will be appreciated, in order to avoid any problems of fraud, it is essential that control word information or, indeed, any other information used in decrypting and descrambling a transmission, is never transmitted in a clear form over the link 51.

There will now be described with reference to Figures 5 and 6, a method for enabling such a secure communication link to be implemented.

For the sake of clarity, all encryption operations using a public/private key algorithm are indicated by means of the symbol f_a, whilst all operations using a symmetric algorithm are indicated by the symbol f_s. Decryption operations are indicated as $f_a^{?2}$ or $f_s^{?2}$.

Private/public keys pairs may be generated in accordance with any suitable asymmetric encryption algorithm such as RSA or Diffie-Hellman. Symmetric keys may be used with algorithms such as DES. In some cases, custom symmetric algorithms may also be used.

Referring to Figure 5, the smart card 52 for the decoder 50 is personalised with a public key KpubMan shown at 65 and equivalent to the public key associated with a private management key KpriMan shown at 61. In practice, all smartcards 52 intended for use with dependent or slave decoders will include the key KpubMan.

This personalisation step will be normally carried out in private at the headquarters of the system manager, either at the moment of first personalisation of the card (if it is already envisaged to provide a second decoder) or when a user demands the inclusion of a second decoder in his subscription.

Subsequently, the system manager possessing the secret private key KpriMan shown at 61 will communicate in a dedicated EMM message 62 a certificate Ct(KpubT) shown at 63. The certificate is prepared by encrypting a public key KpubT with the private manager key KpriMan. The EMM further includes a private key KpriT shown at 64 and stored together with the certificate Ct(KpubT) in the non-volatile memory of the smart card 30.

This EMM is itself encrypted in the normal manner for EMMs dedicated to one decoder using appropriate transmission or exploitation keys, such that only the

decoder 12 and card 30 may decrypt this EMM message.

At the moment when the two decoders are put in communication via the IEEE 1394 link 51, the smart card 30 sends the certificate Ct(KpubT) to the smart card 52 as shown at 66. Using the public key KpubMan, the card decrypts the certificate at 67 to obtain the public key KpubT as shown at 68. This public key KpubT will thereafter be uniquely associated with the pairs of decoders 12, 50 and cards 30, 52.

The card 52 thereafter generates a random key value Ks shown at 69. As will be described, this random key is later used as a session key in conjunction with a symmetric algorithm to encrypt messages communicated in both directions between the cards 30, 52. A new session key value may be generated at every subsequent re-connection of the decoder 50 and card 52 in the system, i.e. every time the decoder 50 is switched on by a user, or at every viewing session, for example, of a pay per view film.

The symmetric key Ks is encrypted at 70 using the public key KpubT and the encrypted value sent at 71 to the smart card 30. The card 30 decrypts the message at 73 with the private key KpriT and stores the session key value at 72. As will be understood, in view of the nature of private/public encryption algorithms the encrypted message may only be decrypted by a card possessing the private key KpriT, that is, by the card 30.

As described above, the cards 30, 52 are programmed by the same system manager who embeds or communicates the values KpriT, Ct(KpubT) and KpubMan to the respective cards 30, 52. In a further realisation (not shown) a second layer of authorisation may be provided using a system private key KpriSystem. In this realisation, a certificate Ct(KpubMan) comprising the key KpubMan encrypted by KpriSystem is stored in the card 30.

In such a realisation, the card 52 further possesses a secondary system public key KpubSystem. In operation, the card 30 sends the encrypted value of certificate

Ct(KpubMan) to the card 52 which decrypts this message using KpubSystem to obtain KpubMan. Thereafter, the steps are the same as above, with the card 52 using the key KpubMan to obtain KpubT etc.

Turning now to Figure 6, the steps involved in the secure communication of control word information from the card 30 to the card 52 will now be described.

In normal operation, the slave decoder 50 and card 52 receive a scrambled transmission together with the encrypted ECM messages containing the control word information necessary to descramble the transmission. These ECM messages are passed at 75 via the IEEE 1394 link to the master decoder and card 12, 30. Alternatively, the ECM messages for a transmission that will be displayed via the slave decoder may be received directly by the master decoder and card 12, 30.

The card 30 then carries out at 76 a standard verification step to check that one or both of the decoders have the rights to access this transmission. In the event that the decoders do not have the necessary rights the "non-valid" message 77 is returned to the decoder and card 50, 52 and the process stops.

Assuming the subscriber possesses the necessary rights, the ECM message shown at 79 and containing the encrypted control word CW is then decrypted at 80 using the monthly exploitation key Kex shown at 81 associated with the system manager or operator.

The clear value of the control word shown at 81 is then re-encrypted at 82 using the previously obtained session key Ks shown at 83. As will be understood, the encryption algorithm used at 82 for the re-encryption of the control word need not correspond to that used at 80 and, indeed, for security reasons a different algorithm may be used. Conveniently, a custom algorithm proprietary to the system manager may be used for steps relating to the exploitation key Kex including the decryption step shown at 80 and a generic algorithm such as DES used for the encryption of session messages shown at 80.

In some cases, additional information, such as copyright notification information may be introduced between the steps 81 and 82, such that the control word CW and this additional information are encrypted by Ks and sent to the second decoder and card. The presence of such information is more important in cases where the second decoder is capable of recording the data or of passing the information to a recorder. The copyright notification may be used as a flag to prevent the second decoder from recording the data or from recording and playing back the data an infinite number of times, for example.

The encrypted control word is returned to the decoder 50 and card 52 as shown at 83. Using the equivalent session key Ks shown at 84, the card decrypts the message at 85 to obtain the control word in clear shown at 86. Thereafter, this control word value is used by the decoder and card 50, 52 to descramble the associated section of a transmission for subsequent display on the associated television display 55.

In some cases, it may be envisaged that the decoder 50 and card 52 may wish to pass information to another audiovisual device, such as a VCR. In such an example, the decoder 50 and card 52 may be supplied with the necessary private keys to assume the role of a "master" device and the same operations carried out, mutatis mutandis, between the decoder and the other device to set up a secure link.

Whilst the above description has focused on the validation and communication of information in relation to a pair of decoders, the invention may equally expanded to cover a series of interconnected decoders, for example, a single master decoder possessing a plurality of private transport keys KpriT for decryption of messages from a plurality of dependent decoders each possessing its equivalent public key KpubT.

Furthermore, whilst the data communicated from the decoder to the recorder comprises the control word in the described example other information may be passed via this link, even including information not related directly to descrambling a transmission.

Equally, the same principles as set out above may be applied to communications between other digital audiovisual devices connected in a network, such as digital VCRs, digital televisions or any combination of such devices. For example, referring to Figure 7, the elements of an access control system for recordal and replaying of scrambled transmission will now be described.

Decoder and Recorder Configuration

As before, a decoder 12 receives scrambled broadcast transmissions via a receiver 11. The decoder includes a portable security module 30, which may conveniently take the form of a smart card, but which may comprise any other suitable memory or microprocessor device. The decoder 12 includes a modem channel 16, for example, for communicating with servers handling conditional access information and is also adapted to pass descrambled audiovisual display information, e.g. via a Peritel link 53, to a television 13. The system additionally includes a digital recorder 100, such as a DVHS or DVD recorder, adapted to communicate with the decoder, for example, via an IEEE 1394 bus 101. The recorder 100 receives a digital recording support (not shown) on which information is recorded.

The recorder 100 is further adapted to function with a portable security module 102 containing, inter alia, the keys used to control access to the replaying of a recording. The portable security module may comprise any portable memory and/or microprocessor device as is conventionally known, such as a smart card, a PCMCIA card, a microprocessor key etc. In the present case, the portable security module 102 has been designated as a SIM card, as is known from the field of portable telephones.

The digital recorder 100 includes a direct link 104 to the display 13. In alternative realisations, digital audiovisual information may be passed from the recorder 100 to the decoder 12 prior to display. Equally, whilst the elements of decoder 12, recorder 100 and display 13 have been indicated separately, it is conceivable that some or all of these elements may be merged, for example, to provide a combined decoder/television set or combined decoder/recorder etc.

Similarly, whilst the invention will be discussed in relation to the recording of audiovisual broadcast information, it may also conveniently be applied, for example, to broadcast exclusive audio information subsequently recorded on a DAT or minidisc recorder or even a broadcast software application recorded on the hard disc of a computer.

Secure Communication between Decoder and Recorder

As set out in the introduction, it is known from prior art proposed systems to re-encrypt the control word associated with a scrambled transmission with a recording key and to store the re-encrypted control word on the recording support with the scrambled transmission. Unlike the exploitation key associated with encryption and decryption of the original transmission, the recording key may be an unchanging key associated with this particular recording so as to enable the recording to be played back at any time in the future.

As will be seen from the overview of Figure 7, in order to enable independence of the recording elements of the system from the decoder elements, it is necessary that the recording key be associated with the recorder 100, for example, by storing the key in a security module associated with the recorder such as the portable security module SIM card 102. Otherwise, if the key is permanently stored at decoder 12 or smart card 30 it will not be possible for a recorder to play back a recording in the absence of the decoder.

In order to do this it will be necessary to pass certain information between the decoder 12 and the recorder 100 along the link 101. This information may be, for example, decrypted control word information that may be then re-encrypted by use of a recording key at the digital recorder. Alternatively, control word information may be encrypted by a recording key generated by the decoder, this recording key then being sent to the recorder for storage.

In all cases it is necessary to ensure a securised link between the decoder and

recorder. Unfortunately, the independence of activities between a broadcast system manager responsible for the decoder and a manufacturer of recording equipment responsible for the recorder may lead to a number of problems regarding the provision of encryption keys for this purpose.

For example, a broadcast operator may not place sufficient confidence in the integrity of security at the manufacturing site of a recorder to entrust the manufacturer with, for example, a secret symmetric algorithm key needed by the recorder security module 102 to decrypt communications encrypted using the equivalent key held by the decoder security module 30.

Furthermore, the separation of activities may make it impractical to envisage a situation in which the recorder security module 102 is sent to a broadcast system manager for personalisation with the appropriate keys. For this reason, it is necessary to envisage a solution which allows the greatest independence of operation for the decoder and recorder.

Figure 8 shows in schematic form a method of setting up a secure communication link between the decoder and recorder security modules 30, 102 that overcomes these problems.

For the sake of clarity, all encryption/decryption operations using a public/private key algorithm are indicated by means of the symbol f_a in a hexagon, whilst all operations using a symmetric algorithm are indicated by the symbol f_s in an oval.

As shown in Figure 5, the recorder card 102 is prepared by the recorder manufacturer using a system certificate CtKeyRec shown at 120 that is communicated to the recorder manufacturer by the broadcast system manager. As is shown at 121, this certificate corresponds to a manufacturer public key KpubMan encrypted by a broadcaster system private key KpriSystem. The private key KpriSystem is unique to and held exclusively by the system manager and it is not possible to derive this key value from the certificate CtKeyRec even if the value KpubMan is known.

As will become clearer from the description below, the system certificate CtKeyRec which includes the manufacturer key KpubMan serves as a guarantee by the broadcast operator of the integrity of the security of the key system of the manufacturer and, notably, the validity of the key KpubMan. The certificate is generated once only. In this certifying operation, the manufacturer communicates the key KpubMan to the broadcast system manager, who encrypts the key KpubMan using the private key KpriSystem and returns the system certificate CtKeyRec. Thereafter, the manufacturer configures all recorder security modules to include the certificate CtKeyRec during the personalisation step of the recorder security modules.

The key KpubMan itself corresponds to a public key of a private/public key pair associated with the identity of and unique to the recorder manufacturer or source of the recorder. The corresponding private key KpriMan is held exclusively by the recorder manufacturer and is not known even to the broadcast system manager. The key KpriMan is itself used to generate a device certificate CtKeySIM shown at 122. This certificate, which is unique to the recorder security module, corresponds to a recorder security module key KpubSIM encrypted by the private manufacturer key KpriMan.

The key KpubSIM equally corresponds to a public key of a private/public key pair associated with the identity of and unique to the recorder device. This key and the corresponding private key KpriSIM are generated by the recorder manufacturer. As shown, the private key KpriSIM is stored in the recorder security module at 124, preferably at the moment of manufacture of the chip itself.

In the event that an encrypted communication is to be set up between the decoder and the recorder, for example, associated with the recording of a transmission received by the decoder, the system certificate CtKeyRec is transmitted from the recorder security module 102 to the decoder security module 30 as shown at 126.

The decoder security module 30 includes the broadcast system public key KpubSystem shown at 125 and stored in the card 30 during personalisation by the

broadcast system manager. Using the system key KpubSystem, the decoder security module decrypts at 127 the certificate CtKeyRec in order to obtain the manufacturer public key KpubMan.

In the case of a security breach associated with the recorder source, the security module 30 can be programmed to reject certain manufacturer public key values obtained after the decryption step 127. Otherwise, the key KpubMan is stored at 128 and will be used in the next decryption steps.

As shown at 129, the recorder security module 102 then communicates the device certificate CtKeySIM, unique to that recorder security module, to the decoder security module 30. Using the manufacturer public key KpubMan, the decoder security module 30 decrypts at 130 the recorder security module public key KpubSIM.

This public key is stored at 131 in the decoder security module 30 and is then used in the encryption and communication of a session key value. This session key value, which in this example corresponds to a random number value usable by a symmetric encryption/decryption algorithm, is generated at 132, encrypted at 133 by the recorder security module public key KpubSIM and then communicated to the recorder security module at 134.

As will be understood, in view of the nature of public/private key algorithms, this encrypted message may only be decrypted using the unique private key KpriSIM stored at 124 in the recorder security module. Decryption of the message at 135 leads to the extraction of the session key at 136.

Thereafter, each security module 30, 102 will possess a copy of the symmetric session key at 137, 138 for use in encryption and decryption of bi-directional messages. As mentioned above, the session key is used in combination with a symmetric algorithm and equal security is provided for messages in either direction. Other embodiments not requiring bi-directional communication and using an asymmetric algorithm may be envisaged.

As shown in Figure 8, the session key is used in this embodiment to communicate control word information from the decoder to the recorder. In particular, an ECM message 139 associated with the scrambled transmission is received and decrypted by the decoder security module to obtain the clear value of the control word 140 together with any other information contained therein. This control word is then re-encrypted at 141 using the session key stored at 137, and the resulting encrypted message communicated at 142 to the recorder security module 102.

Using the session key stored at 138, the recorder security module decrypts the message at 143 to obtain the clear value of the control word at 144. The control word is then re-encrypted at 145 using a recording key generated internally by the recorder security module and stored at 146. The new ECM comprising this re-encrypted control word and any other information is then recorded on the recording support 147 together with the originally scrambled transmission. Upon playback of the recording, the recorder security module 102 will use the recording key value stored at 146 to decrypt the ECM so as to obtain the control word value to be used in decrypting the scrambled transmission prior to display.

In order to provide a safeguard copy, the recording key may be communicated to the decoder using the session key. The recording is thereafter stored in the decoder security module as a backup in the event of damage or loss of the recorder security module.

The private/public keys pairs KpriSIM, KpubSIM, KpriMan, KpubMan, KpriSystem and KpubSystem may be generated in accordance with any suitable asymmetric encryption algorithm such as RSA or Diffie-Hellman. Equally, the session key and recording key may correspond to key values usable with any suitable symmetric encryption/decryption algorithm such as DES.

As will be understood, alternative realisations of the above embodiment are possible. In the case, for example, where the same system manager is responsible for personalising managing both decoder and recorder security modules, the initial step

of authentification using the system certificate CtKeyRec may be omitted, such that the value of KpubMan is directly inserted in the decoder module at 128.

Furthermore, in the case where the responsibility to ensure integrity of security of transmitted and recorded emissions rests with the manufacturer of the recorder, some or all of the roles of the decoder security module and recorder security module may be completely reversed, such that the recorder manufacturer certifies a public key provided by the broadcast system operator, the recorder is responsible for initiation of communication, generation of a session key etc.

It will also be appreciated that, below the level of the generation of a session key, any number of possibilities for communication of information for use in recording may be envisaged. For example, whilst the data communicated from the decoder to the recorder comprises the control word in the described example it may be envisaged to decrypt and re-encrypt audiovisual data itself before communication to the recorder card. Alternatively, or in addition, the recording key may be generated at the decoder security module and communicated to the recorder security module.

Finally, whilst the above description has focused on the validation and communication of information in relation to single sources of recorders or decoders, the invention may equally expanded to cover multiple decoder and/or recorder sources. For example, a recorder security module may include a plurality of system certificates CtKeyRec associated with a plurality of broadcast system managers. Equally a decoder security module may be adapted to handle a plurality of recorder manufacturer management keys KpubMan obtained after the first verification step is carried out.

Whilst the use of a changing session key increases the level of security, other realisations can be envisaged where a constant session key is used or where the public/private keys KpubSIM/KpriSIM are used to directly encrypt information communicated from the one device to the other device. The session key may itself comprise a private/public key pair.

CLAIMS

1. A method of providing secure communication of information between at least a first and second digital audiovisual device and characterised in that the second device receives a certificate comprising a transport public key encrypted by a management private key, the second device decrypting the certificate using an equivalent management public key and thereafter using the transport public key to encrypt information sent to the first device, the first device using an equivalent private key to decrypt the information.

2. A method as claimed in claim 1 in which the transport private/public key pair are uniquely associated with the first and second device.

3. A method as claimed in any preceding claim in which the encrypted information sent by the second device comprises a session key.

4. A method as claimed in claim 3 in which the session key is a key generated by the second device and usable in conjunction with a symmetric encryption algorithm.

5. A method as claimed in claim 3 or 4 in which the session key is used by the first device to encrypt control word information subsequently communicated to the second device.

6. A method as claimed in claim 5 in which the second device decrypts the control word information using the equivalent session key and thereafter descrambles the section of a scrambled transmission associated with this control word.

7. A method as claimed in any preceding claim in which the first and second devices comprise a respective first and second portable security module.

8. A method as claimed in any preceding claim in which the second device receives a system certificate comprising the management public key encrypted by a system

private key, the second device decrypting the system certificate using a system public key so as to obtain the management public key used thereafter to decrypt the encrypted transport public key.

9. A method as claimed in any preceding claim in which the communication link between the first and second devices is implemented by a bus connection.

10. A method as claimed in any preceding claim in which the first and second digital audiovisual devices comprise a first and second decoder.

11. A method as claimed in claim 10 in which the first and second decoders are adapted to receive digital television transmissions.

12. A method as claimed in any of claims 1 to 9 in which the first and second digital audiovisual devices comprise a decoder device and a recorder device.

13. A method of providing secure communication of information between a decoder device and a recorder device and characterised in that a first one of the devices communicates to the second device a certificate comprising a device public key encrypted by a management private key, the second device decrypting the certificate using an equivalent management public key and thereafter using the device public key to encrypt information sent to the first device, the first device using an equivalent device private key to decrypt the information.

14. A method as claimed in claim 13 in which the first device communicates to the second device a system certificate comprising the management public key encrypted by a system private key, the second device decrypting the system certificate using a system public key so as to obtain the management public key used thereafter to decrypt the device certificate.

15. A method as claimed in claim 13 or 14 in which the device private/public key pair are uniquely associated with the identity of the first device.

16. A method as claimed in any of claims 13 to 15 in which the management private/public key pair are uniquely associated with the source of the first device.

17. A method as claimed in claim 14 in which the system private/public key pair are uniquely associated with the source of the second device.

18. A method as claimed in any of claims 13 to 17 in which the encrypted information sent by the second device comprises a session key.

19. A method as claimed in claim 18 in which the session key is a key generated by the second device and usable in conjunction with a symmetric encryption algorithm.

20. A method as claimed in claim 18 or 19 in which the session key is used by the decoder device to encrypt control word information subsequently communicated to the recorder device.

21. A method as claimed in claim 20 in which the recorder device may decrypt the control word information using the equivalent session key and thereafter re-encrypt the control word information using a recording encryption key, the re-encrypted control word information being stored by the recorder device on a recording support medium together with the scrambled transmission data associated with that control word information.

22. A method as claimed in claim 21 in which the recorder device communicates to the decoder device a copy of the recording encryption key.

23. A method as claimed in claim 22 in which the recorder device communicates a copy of the recording encryption key as encrypted by the session key.

24. A method as claimed in any of claims 13 to 23 in which at least one of the recorder device and decoder device comprises at least one portable security module.

25. A method as claimed in any of claims 13 to 24 in which the first device corresponds to a recorder device and the second device to a decoder device.

26. A method as claimed in any of claims 13 to 25 in which the decoder device is adapted to receive a digital television transmission.

27. A method of providing secure communication of information between at least a first and second digital audiovisual device substantially as herein described.

Fig.1.

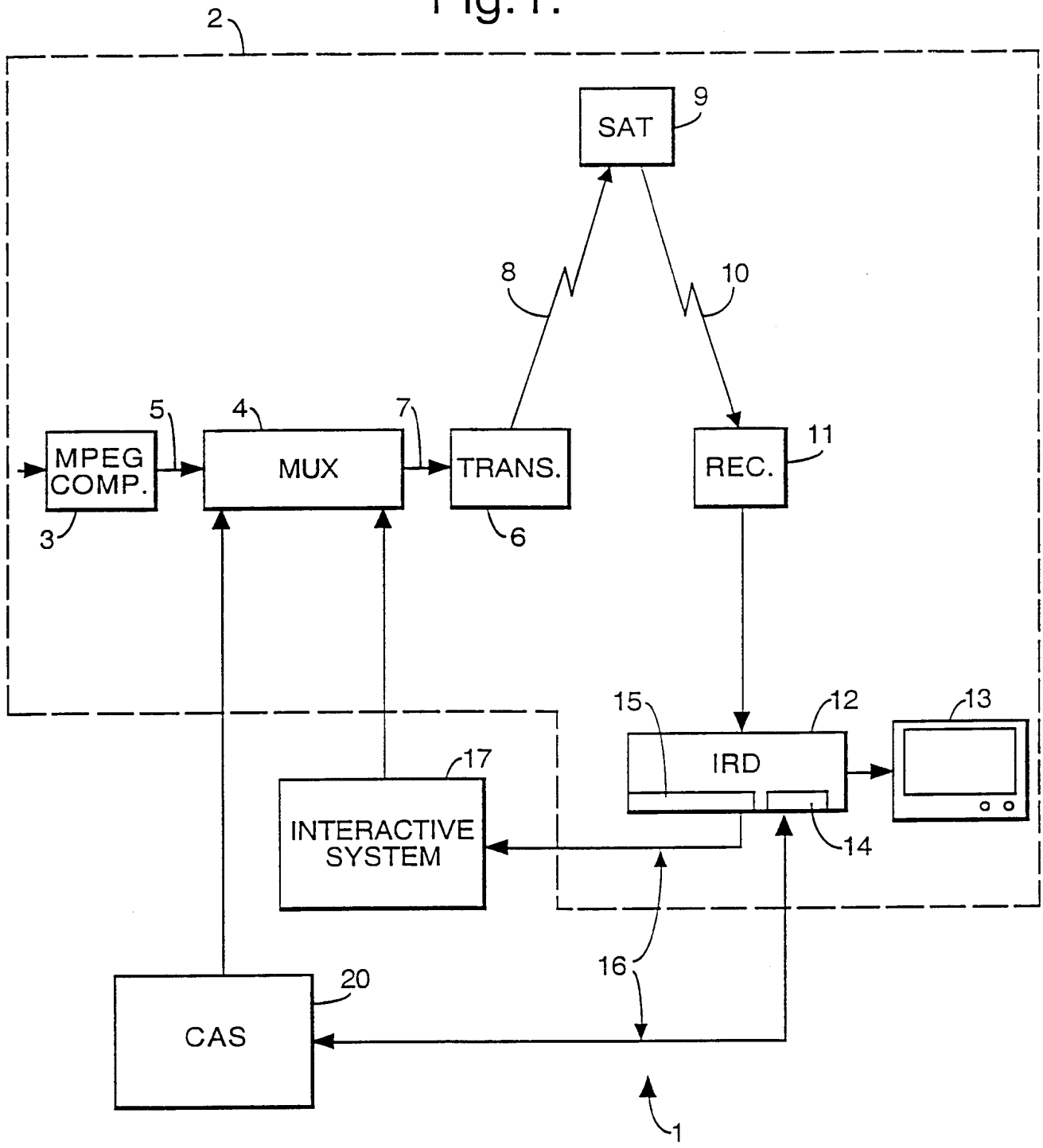

2
SAT
9
8
10
5
4
7
MPEG COMP.
MUX
TRANS.
REC.
11
3
6
15
12
13
IRD
17
INTERACTIVE SYSTEM
14
16
20
CAS
1

Fig.2.

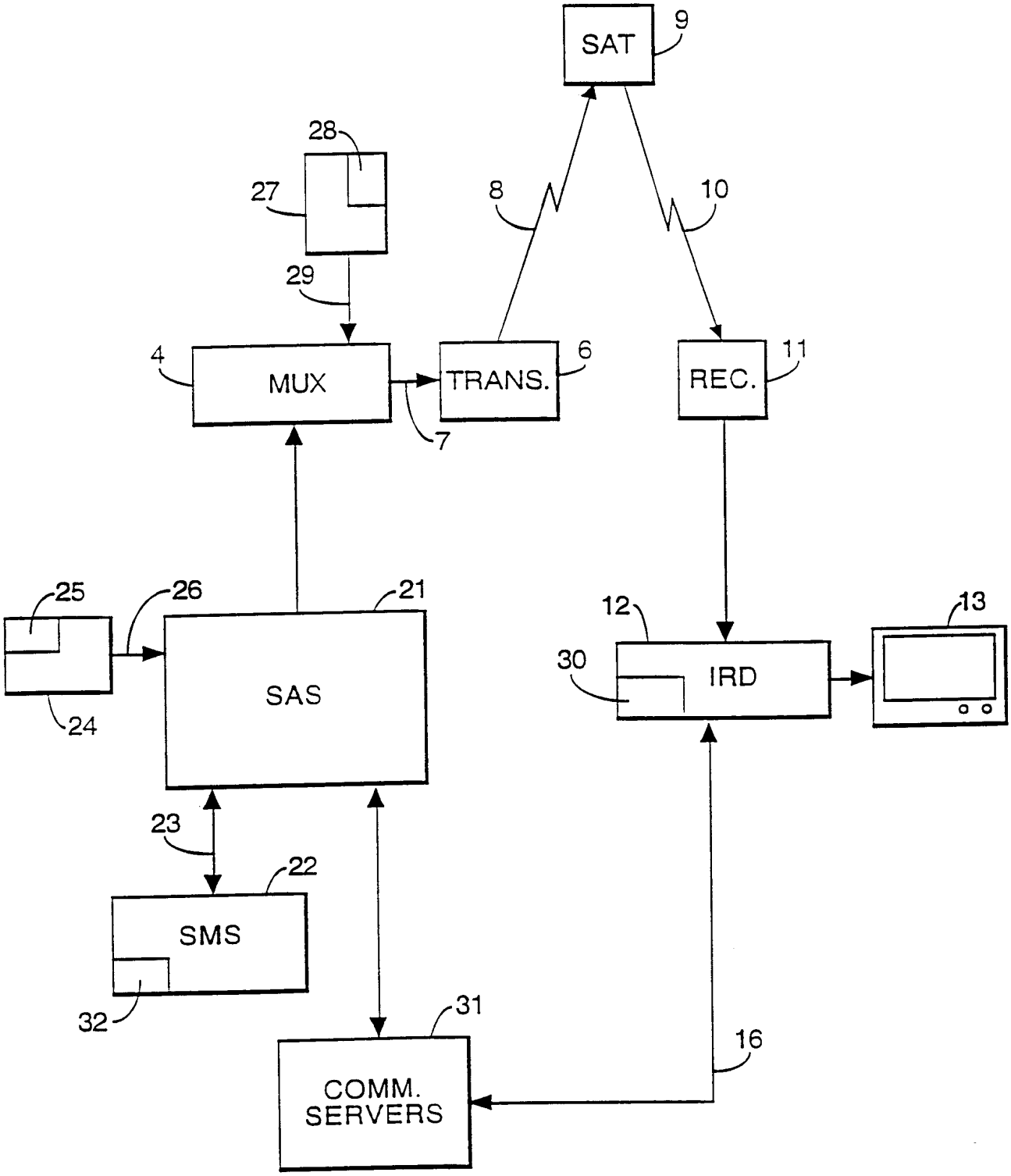
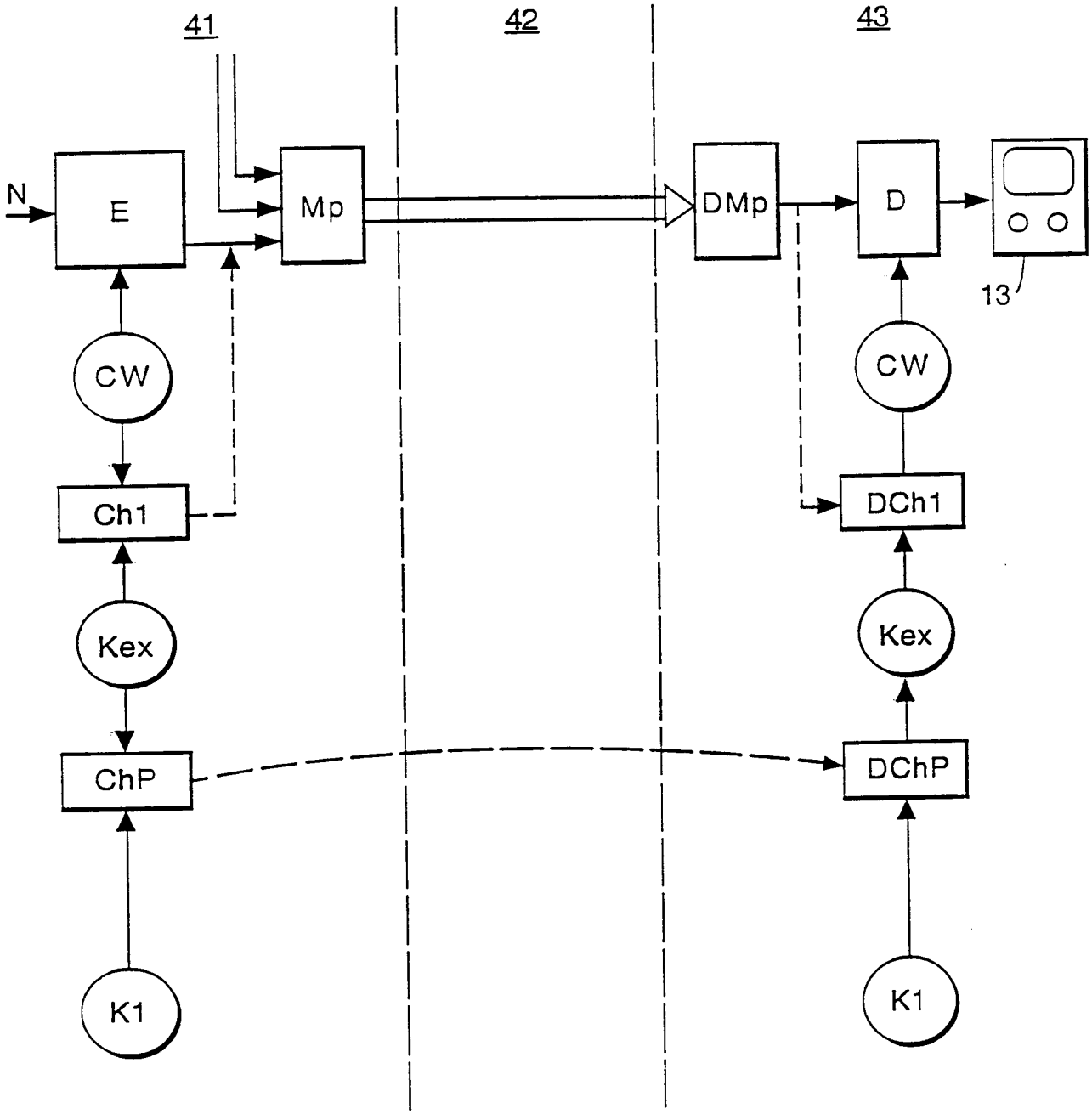

SAT
9
28
27
8
10
29
4
MUX
TRANS.
6
REC.
11
7
25
26
21
12
13
SAS
30
IRD
24
23
22
SMS
32
31
16
COMM.
SERVERS

Fig.3.


41
42
43
N
E
Mp
DMp
D
13
CW
CW
Ch1
DCh1
Kex
Kex
ChP
DChP
K1
K1

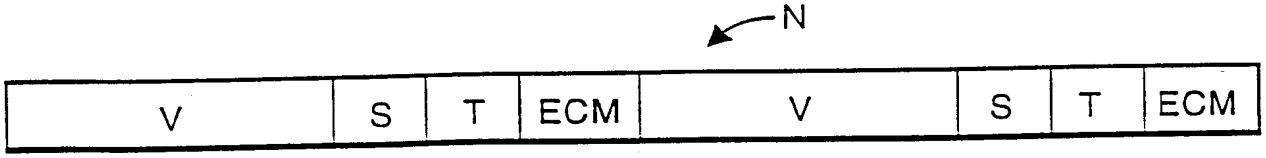

N
V
S
T
ECM
V
S
T
ECM

Fig.4.

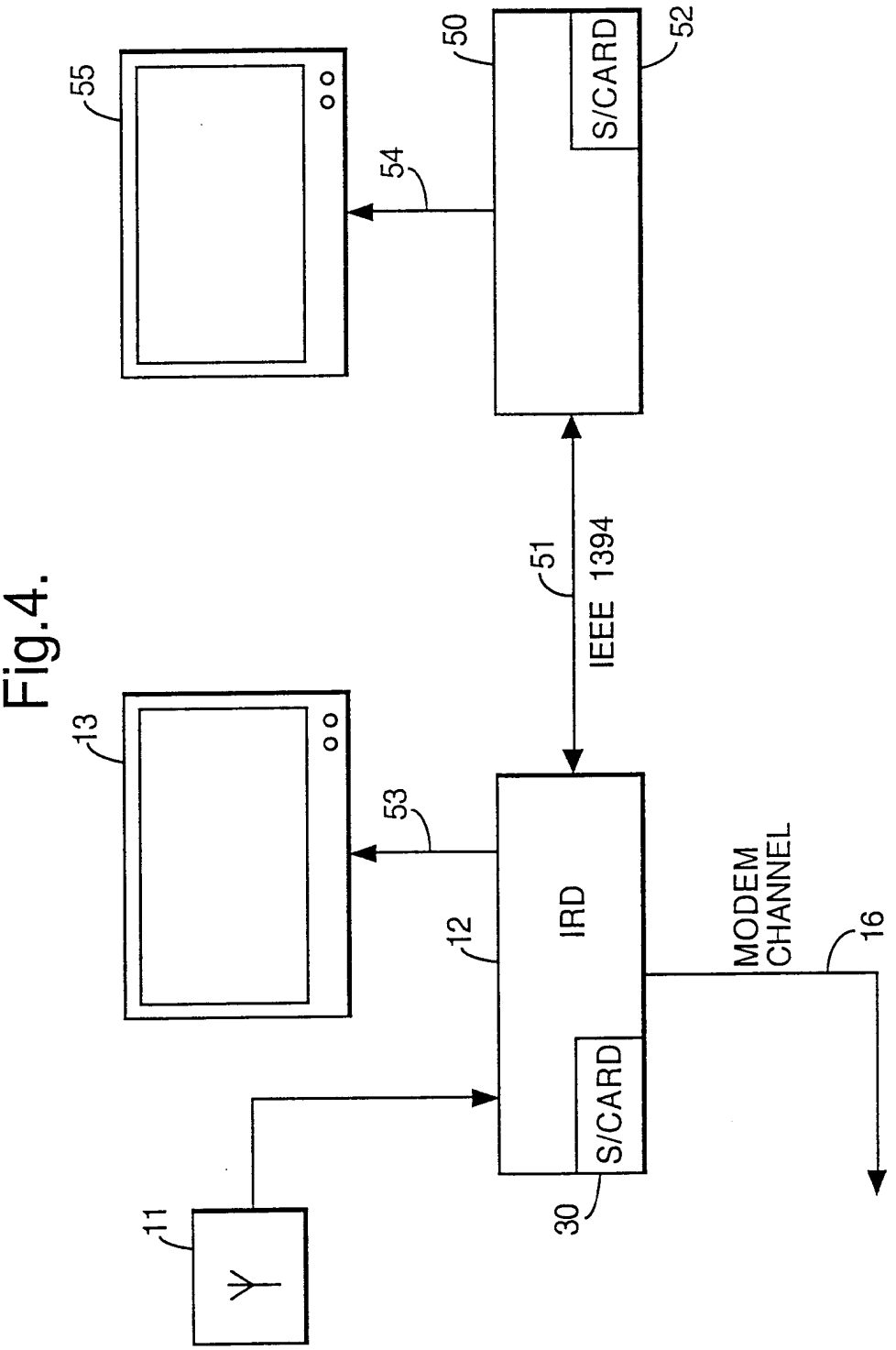

55
50
S/CARD
52
54
51
IEEE 1394
13
53
12
IRD
MODEM
CHANNEL
16
S/CARD
30
11

Fig.5.

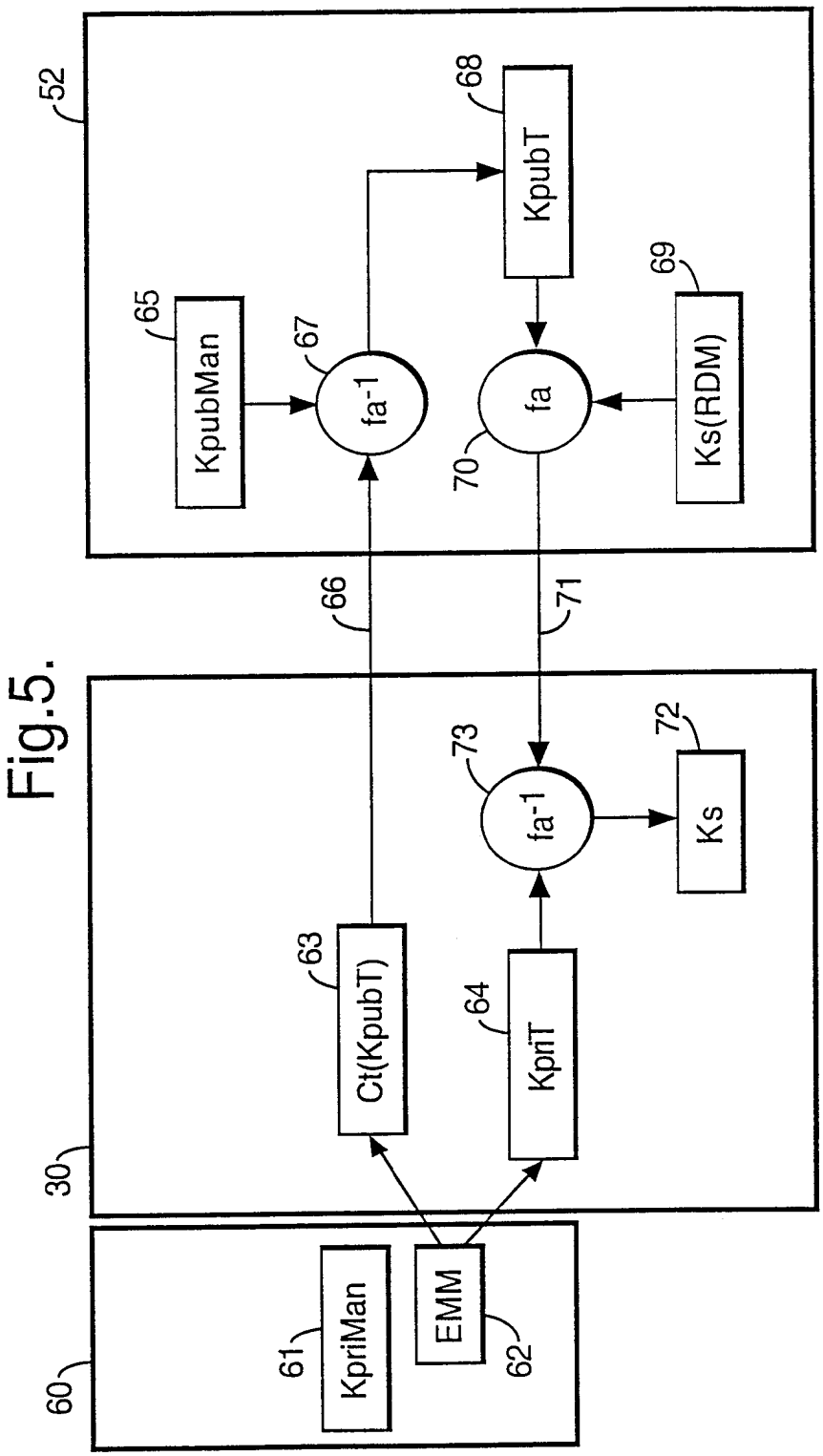

52
68
KpubT
65
KpubMan
67
fa-1
fa
69
Ks(RDM)
70
66
71
30
73
fa-1
72
Ks
63
Ct(KpubT)
64
KpriT
60
61
KpriMan
EMM
62

Fig.6.

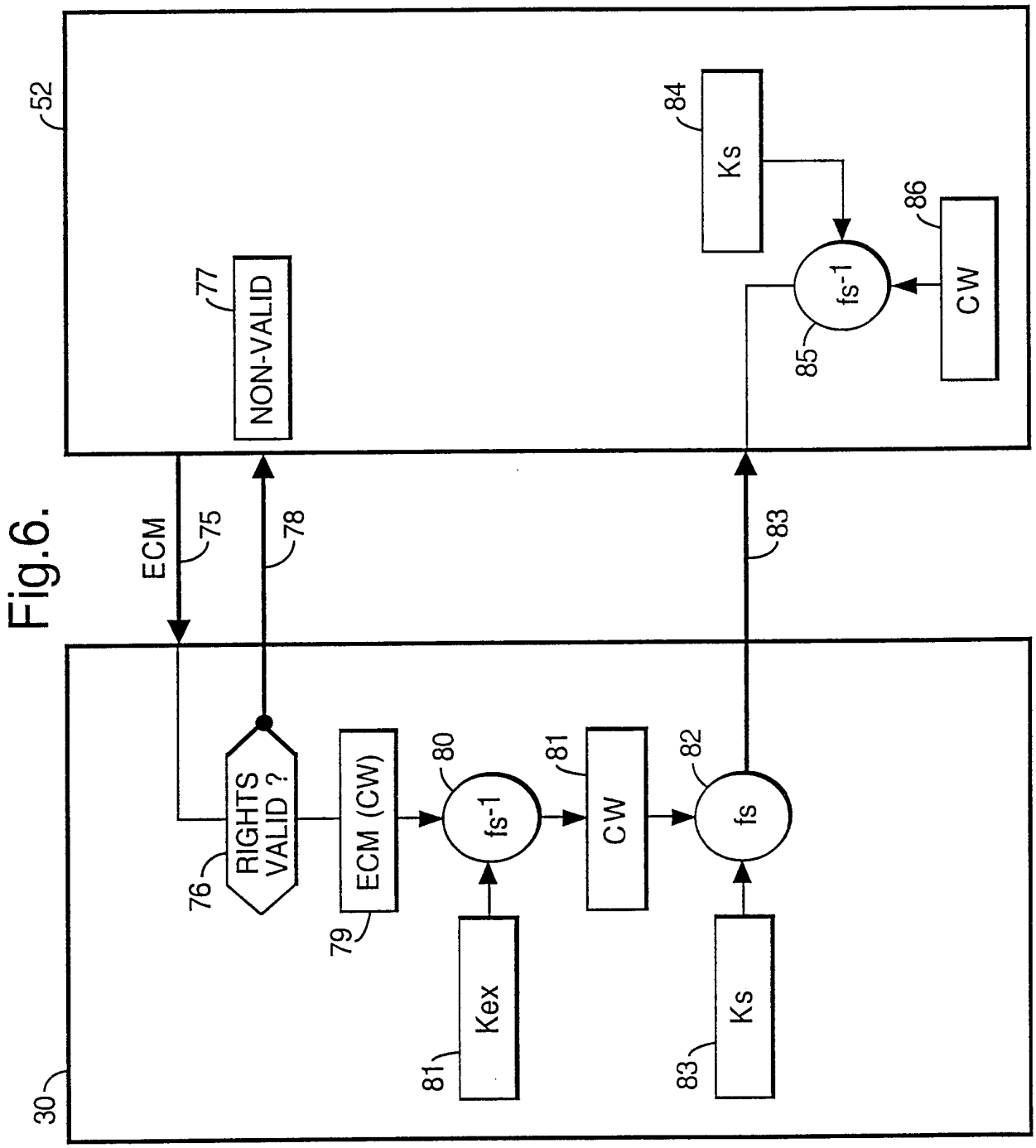

52
84
Ks
86
CW
fs-1
85
77
NON-VALID
ECM
75
78
83
RIGHTS VALID ?
76
ECM (CW)
79
80
fs-1
81
CW
82
fs
Kex
81
Ks
83
30

Fig. 7.

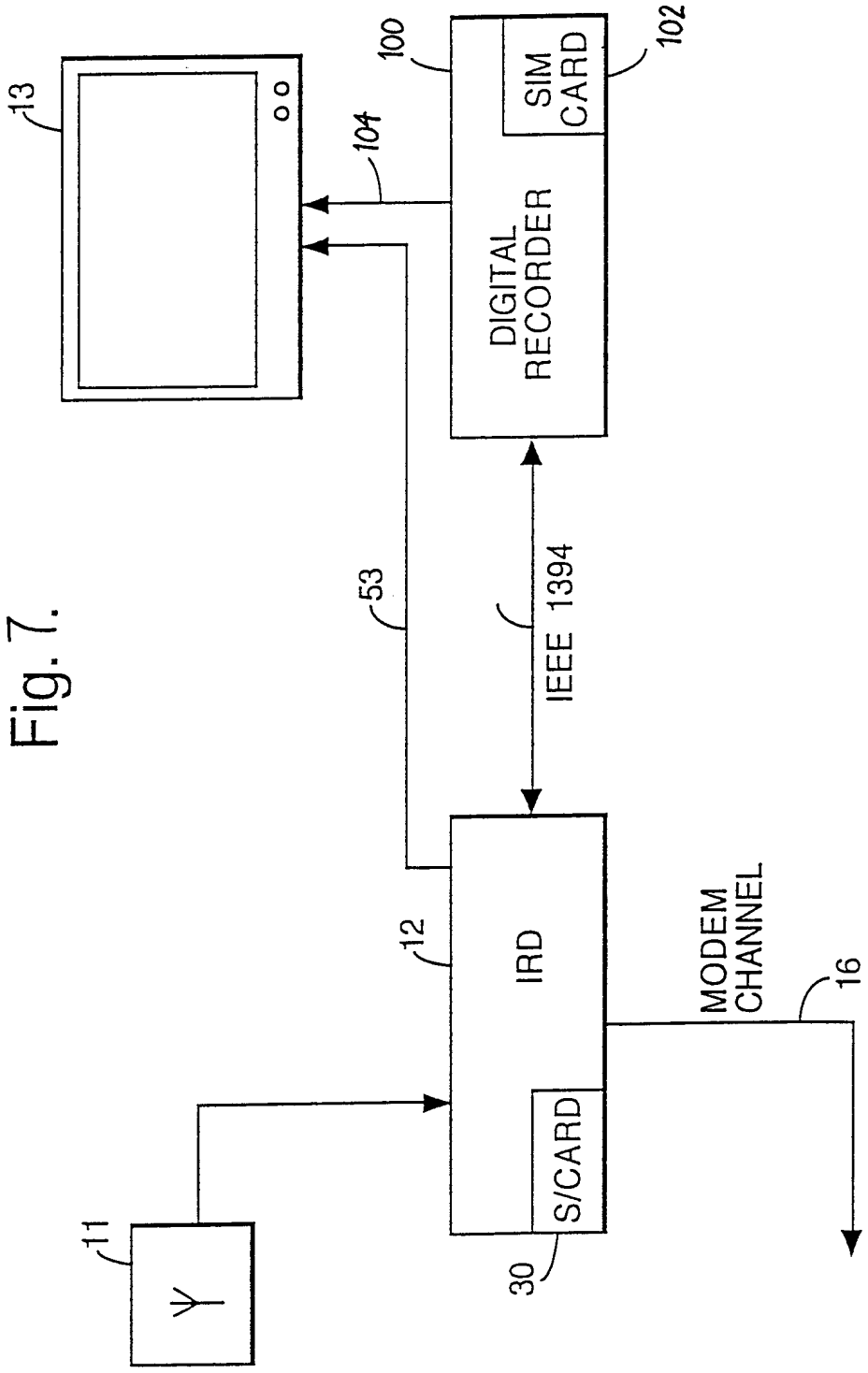
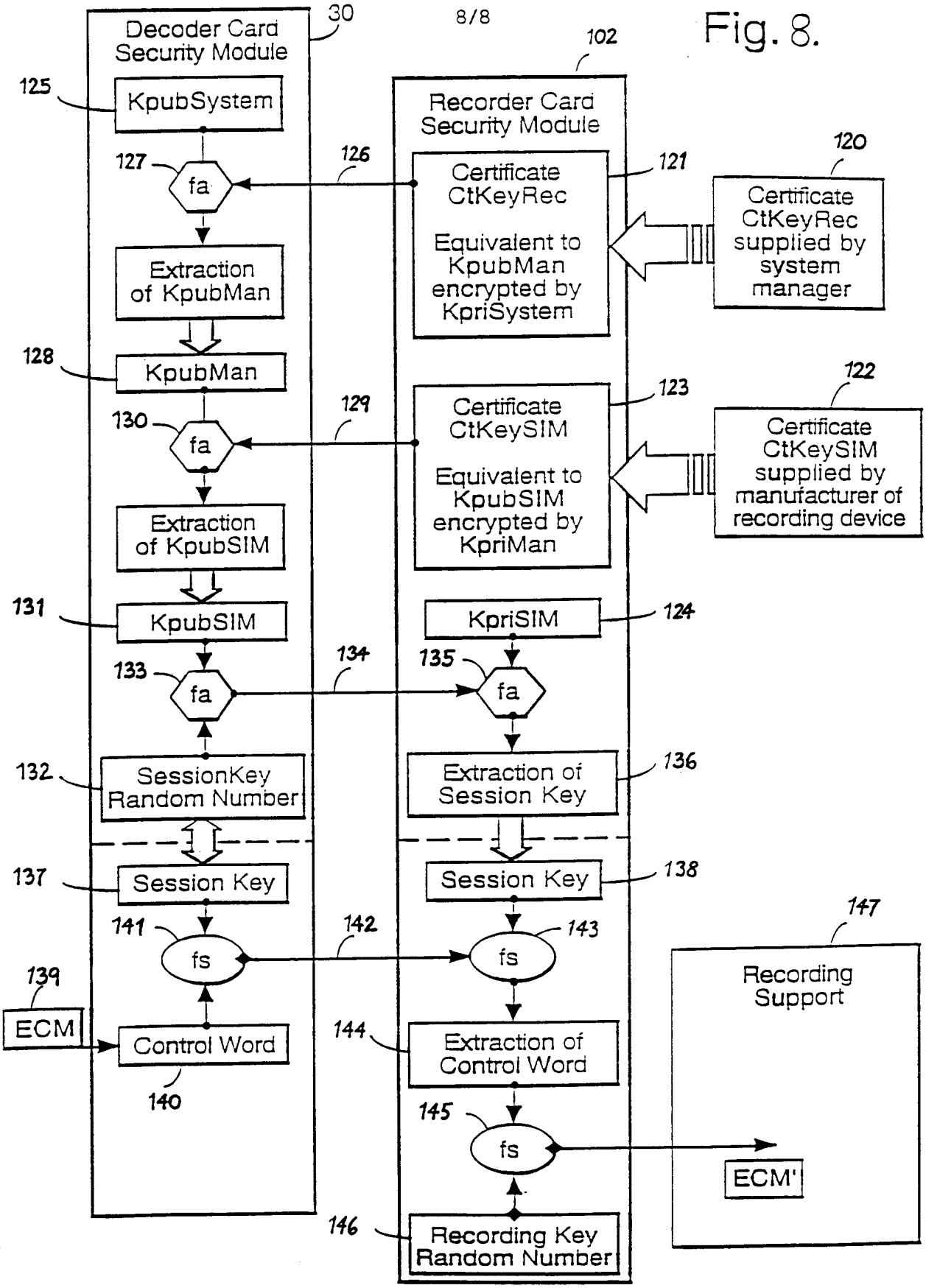

13
100
SIM CARD
102
104
DIGITAL RECORDER
53
IEEE 1394
12
IRD
MODEM CHANNEL
16
S/CARD
30
11

Fig. 8.


Decoder Card Security Module
30
125
KpubSystem
127
fa
126
Extraction of KpubMan
128
KpubMan
130
fa
129
Extraction of KpubSIM
131
KpubSIM
133
fa
134
132
SessionKey Random Number
137
Session Key
141
fs
142
139
ECM
Control Word
140
Recorder Card Security Module
102
Certificate CtKeyRec
Equivalent to KpubMan encrypted by KpriSystem
121
120
Certificate CtKeyRec supplied by system manager
Certificate CtKeySIM
Equivalent to KpubSIM encrypted by KpriMan
123
122
Certificate CtKeySIM supplied by manufacturer of recording device
KpriSIM
124
135
fa
Extraction of Session Key
136
Session Key
138
143
fs
144
Extraction of Control Word
145
fs
146
Recording Key Random Number
147
Recording Support
ECM'

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/IB 99/01323

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 97 38530 A (DIGCO B V ;RIX SIMON PAUL ASHLEY (ZA); GLASSPOOL ANDREW (GB); DAVI) 16 October 1997 (1997-10-16) page 1, line 19 - line 26 page 4, line 1 -page 5, line 10	1,3,5,6, 12,13, 26,27 10,11, 24,25
Y A	US 5 748 732 A (LE BERRE JACQUES ET AL) 5 May 1998 (1998-05-05) column 1, line 17 -column 2, line 16 column 3, line 23 - line 35 column 3, line 64 -column 4, line 43	10,11 9

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 October 1999	05/11/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Sindic, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/IB 99/01323

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 97 35430 A (NEWS DATACOM LTD ;TSURIA YOSSEF (IL)) 25 September 1997 (1997-09-25)	10,11
A	page 3, line 1 -page 4, line 16	9
Y	"ENCRYPTION OF INFORMATION TO BE RECORDED SO AS TO PREVENT UNAUTHORIZED PLAYBACK" RESEARCH DISCLOSURE, no. 335, 1 March 1992 (1992-03-01), page 219 XP000301128 ISSN: 0374-4353 the whole document	24,25
A	FORD W ET AL: "PUBLIC-KEY CRYPTOGRAPHY AND OPEN SYSTEMS INTERCONNECTION" IEEE COMMUNICATIONS MAGAZINE, vol. 30, no. 7, 1 July 1992 (1992-07-01), pages 30-35, XP000307910 page 2, paragraph 5	1,13,27
A	FR 2 732 537 A (CANAL PLUS SA) 4 October 1996 (1996-10-04) page 2, line 12 -page 3, line 23	13,18
A	US 4 633 309 A (LI TONY C ET AL) 30 December 1986 (1986-12-30) column 2, line 36 - line 68	9

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter onal Application No
PCT/IB 99/01323

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9738530 A	16-10-1997	AU 2506397 A	29-10-1997
		CA 2250833 A	16-10-1997
		CN 1215528 A	28-04-1999
		EP 0891670 A	20-01-1999
		HR 970160 A	28-02-1998
US 5748732 A	05-05-1998	FR 2730372 A	09-08-1996
		EP 0726676 A	14-08-1996
		JP 8251569 A	27-09-1996
WO 9735430 A	25-09-1997	IL 117547 A	14-07-1999
		AU 1317597 A	10-10-1997
		EP 0826288 A	04-03-1998
		GB 2311451 A,B	24-09-1997
FR 2732537 A	04-10-1996	NONE	
US 4633309 A	30-12-1986	CA 1250656 A	28-02-1989